VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ
WIRELESS NETWORK

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — BORIS ŠUMAJ
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. MILOŠ KOCH, CSc.
SUPERVISOR

BRNO 2011

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2010/11
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Boris Šumaj

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Problematika bezdrátových sítí

v anglickém jazyce:

Wireless Network

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BARKEN,Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. 1.vyd. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
BRISBIN, Shelly. Wi-fi: postavte si svou vlastní wi-fi síť. 1.vyd. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.
KöHRE,Thomas. Stavíme si bezdrátovou síť Wi-fi. 1.vyd. Brno: Computer Press, 2004. 296 s. ISBN 80-251-0391-9.
ZANDL,Patrick. Bezdrátové sítě WiFi : praktický průvodce. 1.vyd. Brno:Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Vedoucí bakalářské práce: doc. Ing. Miloš Koch, CSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2010/11.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ
L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. RNDr. Anna Putnová, Ph.D., MBA
Děkanka

V Brně, dne 6.2.2011

Abstrakt

Obsahom mojej bakalárskej práce je osvetlenie základnej problematiky bezdrôtových sietí. Podáva prehľad štandardov IEEE 802.11. Tieto štandardy analyzujem so zameraním na ich bezpečnosť a architektúru. Ďalším krokom bude následné vytvorenie bezpečnej podnikovej siete podľa zistených skutočností pre konkrétny podnik.

Abstract

The content of this thesis is to illuminate the basic issues of wireless networks. It gives an overview of IEEE 802.11 standards. I´ll analyze these standards with special emphasis on their security and architecture. The next step will be the subsequent creation of a secure corporate network according to the established facts of a particular company.

Kľúčové slová

WiFi, IEEE 802.11, 802.1x, WLAN, WEP, WPA, WPA2, bezdrôtové siete, bezpečnosť bezdrôtových sietí, architektúra WLAN, SSID, EAP, PEAP, autentizácia, autorizácia, útoky na bezdrôtové siete, warwalking, RADIUS.

Keywords

WiFi, IEEE 802.11, 802.1x, WLAN, WEP, WPA, WPA2, wireless networks, security of wireless networks, architecture of WLAN, SSID, EAP, PEAP, authentization, authorization, attacks at wireless networks, warwalking, RADIUS.

Bibliografická citácia práce

ŠUMAJ, B. *Problematika bezdrátových sítí.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2011. 67 s. Vedoucí bakalářské práce doc. Ing. Miloš Koch, CSc.

Poďakovanie

Týmto by som veľmi rád poďakoval pánovi doc. Ing. Milošovi Kochovi, CSc., vedúcemu mojej bakalárskej práce, za jeho cenné rady a pripomienky, metodickú pomoc a podporu, ktorej som využíval pri spracovaní bakalárskej práce.

Čestné prehlásenie

Prehlasujem, že mnou predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dňa 31. 5. 2011

.....

Boris Šumaj

Obsah

Úvod

Bezdrôtové siete sa v poslednej dobe stali neodmysliteľnou súčasťou našich životov, môžeme sa s nimi stretnúť v práci, škole, či dokonca na verejných miestach ako sú reštaurácie či obchody. Mnohí užívatelia, ktorí využívajú služieb takýchto sietí, často zabúdajú na svoju bezpečnosť, poprípade na bezpečnosť informácií, ktoré prostredníctvom týchto sietí zdieľajú. Z pohľadu bežného užívateľa je veľmi ľahké zabudnúť na skryté možnosti, či určité nedostatky v zabezpečení sietí, nakoľko takýto užívateľ nie je často krát dostatočne informovaný o týchto bezpečnostných rizikách. Neuvedomuje si preto aké, mnohokrát citlivé, dáta v týchto sieťach prúdia. Preto je dôležité venovať sa nielen zabezpečeniu sietí, ale i zabezpečeniu samotných používateľov, ktorí do týchto sietí vstupujú. Tu prichádza na rad bezpečnostná politika, ktorá musí byť striktne stanovená a jej pravidlá sa musia poctivo dodržovať. Takáto politika je vhodná najmä v podnikovom prostredí, kde je potrebné zabezpečiť informácie tak, aby sa k nim neoprávnený užívateľ nedostal. Toho môžeme dosiahnuť nastavením oprávnení užívateľov či použitím antivírových programov, firewallu a ďalších nástrojov počítačovej bezpečnosti.

Vymedzenie problému a ciele práce

Uviesť čitateľa do problematiky bezdrôtových sietí a rozšíriť jeho vedomosti o používaných špecifikáciách IEEE 802.11 používaných pri zostavovaní bezdrôtových sietí, vysvetliť princípy ich použitia a ich vlastnosti. Ďalej zanalyzovať tieto špecifikácie s ohľadom na ich stránku bezpečnosti a architektúry. V praktickej časti vypracujem návrh na vytvorenie podnikovej bezdrôtovej siete s ohľadom na bezpečnosť a zadané požiadavky, čiže výstavba siete s maximálnym prihliadnutím na jej bezpečnosť tak, aby sa mohla vyrovnať metalickej sieti.

1 Teoretické východiská práce

Ako vlastne vznikali bezdrôtové siete? Dôvodom vzniku jednotného štandardu pre bezdrôtové siete bolo zaistiť prepojenie mobilných zariadení, ako sú notebooku či PDA, a ich pripojenie do lokálnych sietí. Názov WiFi, pod ktorým sú bezdrôtové siete označované, vznikol slovnou hrou s slovom HiFi, v porovnaní s High Fidelity, čo znamená „vysoká dôveryhodnosť“, by sa dala chápať skratka k Wireless Fidelity ako „bezdrôtová dôveryhodnosť“. Názov WiFi v skutočnosti nie je skratkou k tomuto výrazu. Výraz WiFi je ochranná známka WiFi Alliance a dnes sa bežne používa ako skratka označujúca siete založené na štandarde 802.11. Pred vznikom štandardu IEEE 802.11 sa musel používať pre tvorbu bezdrôtovej siete hardware od jedného výrobcu. Rôzne normy a špecifikácie hardware u jednotlivých výrobcov znemožňovali kompatibilitu zariadení a rozšírenie bezdrôtových sietí. (18)

1.1 Štandard 802.11

Kvôli týmto nedostatkom sa spoločnosť IEEE[1] (Institute of Electrical and Electronics Engineers) rozhodla vytvoriť zjednocujúcu normu, v roku 1997 tak vznikol prvý štandard z rodiny 802.11. Táto rádiová norma pracovala v bezlicenčnom frekvenčnom pásme 2.4 GHz poskytujúc prenosovú rýchlosť 1-2 Mbps. Protokol pokrýval prvú (fyzickú) a druhú (linkovú) vrstvu modelu ISO/OSI. Na úrovni **linkovej vrstvy boli štandardom 802.11 podľa Lee Barkena[2] definované služby**:

- autentizácia a deautentizácia,
- asociácia, disasociácia a reasociácia,
- privátnosť alebo WEP a
- doručovanie MSDU (Mac Service Data Unit),

[1] *IEEE 802.11, The Working Group Setting the Standards for Wireless LANs* [online]. 2010 [cit. 2010-11-30]. Dostupné z WWW: <http://www.ieee802.org/11/>.
[2] BARKEN, Lee. Wi-Fi: Jak zabezpečit bezdrátovou síť. 2004, s. 28.

a na **úrovni fyzickej vrstvy boli stanovené metódy prenosu dát** DSSS (Direct Sequence Spread Spectrum), FHSS (Frequency Hopping Spread Spectrum) a infračervený prenos. Áno, ako uvádza Lee Barken, protokol 802.11 obsahuje na prekvapenie mnohých i podporu infračervených prenosov a i napriek definovaní tejto implementácie na infračervených zariadeniach nebol doposiaľ vyvinutý žiadny komerčne úspešný produkt, ktorý by nejakým významným spôsobom využíval tejto metódy prenosu dát. (1, s. 28)

1.2 Metódy rádiového prenosu dát

To, ako budú jednotlivé dátové bity prenášané, definuje fyzická vrstva, v ďalších odstavcoch si popíšeme podrobne tieto metódy komunikácie po sieti.

1.2.1 FHSS

FHSS (Frequency Hopping Spread Spectrum) je metóda prenosu dát na fyzickej vrstve pomocou preskakovania frekvencií rozprestretým spektrom. Tento systém sa objavil v patente z roku 1942 nazvanom „Bezpečnostný komunikačný systém“. Jeho myšlienkou bolo vytvoriť systém, ktorý by udržal rádiovo navádzané torpéda na správnom kurze. Princíp je založený na preskakovaní signálu v malom časovom rozmedzí medzi frekvenciami. Rušička tak nemohla zachytiť signál a efektívne ho rušiť, pretože v dobe odhalenia signálu už tento pracoval na inej frekvencii. A tak vznikla metóda FHSS. Preskoky v nej sa riadia dopredu stanoveným obrazom, použitá je sekvencia 78 možných frekvencií, čiže 79 kanálov. Pásmo 2,4 GHz sa rozdelí na samostatné kanály o šírke 1 MHz, a tým pokryje celý rozsah od 2,4 GHz do 2,4835 GHz. Striedavo sa nich vysiela, maximálne však 400 ms na každom kanáli. Nevýhodou je nízka prenosová rýchlosť, a to iba 2 Mbit/s. Výhodou skokového prenosu je možnosť umiestnenia viacerých zariadení na jednom mieste, a to vďaka komunikácie pomocou rôznych sekvencií. (1, s. 29)

1.2.2 DSSS

Naproti tomu tu máme DSSS (Direct Sequence Spread Spectrum), techniku priamej sekvencie na rozprestretom spektre, založenú na použití kanálov, ktorých šírka je 22 MHz. Do bezlicenčného frekvenčného pásma 2,4 GHz, ktoré má rozsah 83,5 MHz, sa zmestia len tri kanály, pretože prekrývajúce kanály sa rušia. To znamená obmedzenie práce iba na tri siete v jednej lokalite, tak aby sa vzájomne nerušili. V ČR podľa rozhodnutia ČTÚ (Český telekomunikačný úrad), všeobecného oprávnenia VO-R/12/08.2005-6, je k dispozícii celkom 13 frekvenčných kanálov. Tri kanály, ktoré sa neprekrývajú sú potom kanál 1, 7 a 13. Naopak v USA je k dispozícii iba 11 kanálov o šírke 22 MHz s odstupom 5 MHz, kvôli užšiemu celkovému rozsahu frekvencií sú potom tri neprekrývajúce sa dostupné kanály 1, 6 a 11. Rozstupy medzi jednotlivými kanálmi sú tu menšie ako u európskych kanálov, je tu preto väčšie riziko ovplyvňovania prenosu medzi kanálmi navzájom. Ku prenosu jednotlivých bitov sa používajú sekvencie, tzv. „chipy“ Dôsledkom je správa prenášajúca sa širším frekvenčným spektrom, a tak je každý dátový bit zastúpený známou sekvenciou. Použitím rôznych sekvenčných kódov nám umožní umiestniť viacero sietí na jednom mieste. Táto modulačná technika je využívaná ako aj v bezdrôtovej technológii WiFi, tak i v navigačných systémoch GPS. Sú pritom využívané tri modulačné metódy, ktoré zaisťujú rôzne rýchlosti prenosu dát. Prvá je metóda DBPSK (Differential Binary Phase-Shift Keying) s diferenciálnym binárnym fázovým posunom kľúča, pri ktorej môžeme dosiahnuť rýchlosti 1 Mbit/s. S druhou metódou DQPSK (Differential Quadrature Phase-Shift Keying) sa oproti prvej sa líši tým že nie je binárna ale kvadratická. Ku kódovaniu dát dochádza pri zmene fáze, a to buď v prenosoch po dvoch (DBPSK) alebo štyroch (DQPSK) fázach. Použitím štyroch bitov namiesto dvoch dosiahneme dvojnásobnej rýchlosti, čiže 2 Mbit/s. Tretia metóda je založená na modulácii signálu metódou DQPSK s pomocou CCK (Complementary Code Keying), čiže kľúčovaním doplnkovým kódom, kde môžeme dosiahnuť rýchlosti 5,5 Mbit/s alebo 11 Mbit/s rozdelením kódu – kódovaním a prenesením väčšieho objemu dát behom každého fázového posunu. (1, s. 30)

1.2.3 DFIr

Ako som už uviedol vyššie, i keď bol infračervený prenos, označovaný ako DFIr (Diffused Infrared), v špecifikácii 802.11 definovaný, komerčne úspešného využitia nenašiel. Síce je tento prenos odolný proti rádiovému rušeniu vďaka tomu, že operuje s frekvenciou v rádoch THz, ale jeho hlavnou nevýhodu a dôvodom, prečo nebol tento prenos využitý, je obmedzený dosah a neschopnosť prechádzať stenami. Hlavne kvôli týmto optickým obmedzeniam sa prestal takmer úplne vyvíjať. Používal sa hlavne v zariadeniach ako sú mobilné telefóny a PDA, kde bol však postupne nahradený a úplne vytlačený prenosom dát pomocou technológie Bluetooth. (5, s. 20)

1.2.4 OFDM

OFDM (Orthogonal Frequency Division Multiplexing) je metóda prenosu založená na prenose dát s paralelným kmitočtovým delením na rôznych nezávislých frekvenciách. Kanály sa prekrývajú, ale vďaka prítomnosti identifikátorov každého kanálu sa znižuje riziko interferencií. Každý kanál tu má šírku 20 MHz a 48 pomocných nosných vĺn pripadajúcich na jeden kanál a v zálohe je 6 ďalších pomocných nosných vĺn zaisťujúcich réžiu prenosu. I táto vrstva má rôzne modulačné metódy pre dosiahnutie rôznych rýchlostí prenosu. Prvá úroveň dosahuje rýchlosti 6 a 9 Mbit/s pri použití DBPSK, druhá úroveň dosahuje 12 a 18 Mbit/s pri použití DQPSK. Tretia môže dosiahnuť 24 a 36 Mbit/s pridaním QAM (Quadrature Amplitude Modulation) k DBPSK. Posledná štvrtá úroveň dosahuje 48 a 54 Mbit/s kombináciou QAM s DQPSK. Modulácia QAM vyjadruje kódovanie dátových bitov na symboly. Modulácia 16-QAM kóduje 4 dátové bity pri použití 16 symbolov na podkanál a modulácia 64-QAM kóduje 16 bitov s použitím 64 symbolov na podkanál. OFDM sa používa i pre prenos signálu v ADSL, bezdrôtových sieťach štandardov IEEE 802.11a/g, WiMAX a štandardoch pre digitálny príjem signálu v televíznych prijímačoch DAB (Digital Audio Broadcasting) a DVB-T (Digital Video Broadcasting - Terrestrial).(2, s. 20)

1.2.5 Technológia MIMO

MIMO (Multiple-Input Multiple-Output) môžeme ľudovo chápať ako metódu viacerých vstupov a výstupov, je to matematický model pre multi-anténne komunikačné systémy, čiže princíp viacerých prijímacích a vysielacích antén. Nemožno ju zaradiť medzi metódy prenosu dát, je však významnou technológiou zefektívňujúcou spektrálne využitie bezdrôtových systémov využitím viaccestnej propagácie. Zvyšuje dosah a priepustnosť pri zachovaní šírky pásma a celkovej vyžarovanej energie, a snaží sa o zníženie počtu prenosových bitových chýb. Metóda SISO (Single-Input Single-Output), v preklade jeden vstup, jeden výstup, sa naproti tomu snaží zamedziť efektu viaccestnej propagácie. Technológia MIMO môže byt využitá v spojení s OFDM metódou ako časť WiMAX štandardu, ktorý bude súčasťou IEEE 802.11n – štandardu vysokej priepustnosti. MIMO technológia bude použitá i v 3G štandardoch, v HSDPA (High-Speed Downlink Packet Access). (11)

1.3 IEEE 802.11b

IEEE 802.11b bola vydaná v roku 1999. Spoločnosť IEEE aktualizovala a vylepšila štandard 802.11, verzia 802.11b používa už len metódu DSSS a môže tak dosahovať rýchlosti 5,5 a 11 Mbit/s, podľa typu použitej modulácie (DBPSK, DQPSK, CCK). Vyšších rýchlostí sa dá dosiahnuť iba s použitím CCK v rámci DQPSK. Ak sú podmienky pre prenos dát zhoršené napríklad silným rušením frekvenčného pásma, 802.11b použije princípu dynamickej zmeny prenosovej rýchosti v závislosti od týchto podmienok, rýchlosť sa tak môže znížiť na 5,5 Mbit/s a až na 1-2 Mbit/s, pri zlepšení podmienok znovu vyšplhá na maximálnych 11 Mbit/s. Pracuje v bezlicenčnom frekvenčnom pásme 2,4000 – 2,4835 GHz pri možnosti použitia 3 neprekrývajúcich sa kanálov, efektívna rýchlosť je tu pritom do 6 Mbit/s a dosah približne 100 m. 2,4 GHz pásmo nepatrí k tým spoľahlivejším, pracujú v ňom totiž rôzne zariadenia ako napríklad bezdrôtové telefóny, pagery, detské elektronické opatrovateľky a podobné rádiové zariadenia. Výhodou naproti tomu je možnosť využitia tohto pásma po celom svete. Pôvodné 1 a 2 Mb karty DSSS založené na starej špecifikácií sú kompatibilné, avšak karty používajúce iba FHSS nie

sú kompatibilné. Prvé výrobky založené na norme 802.11b uviedla na trh spoločnosť Apple pod názvom Air-port. Apple bola tak prvá spoločnosť, ktorá túto normu spopularizovala. Štandard 802.11b je veľmi obľúbený u širokej verejnosti. Nízke náklady, jednoduchosť použitia a kompatibilita zariadení zaistená činnosťou WiFi Alliance dovoľuje tejto špecifikácii rozvíjať sa, preto je najviac rozšírenou na svete. 802.11b však nezaisťuje QoS (Quality of Services), skrýva aj bezpečnostné riziká, na ktoré je treba brať ohľad. Kvôli tomuto IEEE vytvára rôzne doplnky k rodine IEEE 802.11 a tie si opíšeme v kapitole „1.5 Doplnky rodiny 802.11“ a budeme sa im venovať podrobnejšie. (1, s. 32)

1.4 IEEE 802.11a

V roku 1999 bola taktiež vytvorená norma 802.11a, táto je však odlišná od predošlej hlavne tým, že používa metódu OFDM a operuje v pásme 5 GHz, toto pásmo je menej vyťažené a tým pádom menej rušené, to dovoľuje použiť viacero kanálov bez ich vzájomného rušenia, až 8 nezávislých, neprekrývajúcich sa kanálov. Šírka pásma je väčšia ako u 802.11b a iba málo aplikácií usiluje o vstup do tohto pásma. Teoreticky môže poskytovať rýchlosť až do 54 Mbit/s, reálne dosiahnuteľná rýchlosť je okolo 30 až 36 Mbit/s. Štandard je stabilnejší a vyspelejší, dosahuje väčších vzdialeností vďaka väčšiemu povolenému vyžarovaciemu výkonu oproti štandardom 802.11b/g. Medzi nevýhody patrí nemožnosť komunikácie so zariadeniami používajúcimi štandard 802.11b a z neho vytvorených doplnkov, z tejto nekompatibility s inými zariadeniami vyplýva väčšia finančná náročnosť oproti predchádzajúcej norme 802.11b. (1, s. 34)

1.5 IEEE 802.11g

V roku 2002 bol tematickou skupinou 802.11g schválený tretí sieťový štandard IEEE, ktorý rozšíril pôvodnú normu 802.11b. Mala by byť zlučiteľná s doplnkami 802.11d/e/i, ktoré majú zaistiť internacionalizáciu, QoS a bezpečnosť bezdrôtových prenosov v rámci tejto normy. Využíva pásmo 2,4 GHz, prenosová rýchlosť je až 54 Mbit/s, na fyzickej vrstve je použitá technológia OFDM ako

v norme 802.11a. Pre zachovanie kompatibility so zariadeniami pracujúcimi na starších normách ako je 802.11b bola použitá i technológia DSSS a podpora CCK a voliteľne i PBCC, ale ak sa však k sieti pripojí klient s podporou iba 802.11b, rýchlosť celej siete sa zníži, a to rapídne. Ak by na tom istom kmitočte a mieste naraz pracovali 802.11b CCK, 802.11b PBCC a 802.11g OFDM, môže dôjsť ku vzájomnému rušeniu. Spolu s 802.11b patrí štandard 802.11g k najrozšírenejším a väčšina kariet využíva týchto špecifikácií. Vysielací výkon je tu oproti norme 802.11b nižší, preto je hlavné využitie prevažne v domácnostiach a aj v malých podnikoch. (1, s. 36)

1.6 Doplnky rodiny 802.11

IEEE 802.11d

- WiFi štandard nazývaný globálny harmonizačný štandard z roku 2001, vhodný najmä pre systémy, ktoré chcú poskytovať globálny roaming. Využitie nájde v krajinách, kde systémy používajúce iné dodatky rodiny 802.11 nie sú povolené. Jeho definícia zahrňuje požiadavky na fyzickú vrstvu tak, aby uspokojovala regulačné domény nepokryté existujúcimi štandardmi. Odlišnosti sú v povolených frekvenciách, vyžarovacích výkonoch a priepustnosti signálu. Snaží sa eliminovať nutnosť produkcie špecifických produktov pre rôzne krajiny – unifikuje produkty. Princíp protokolu spočíva v prispôsobovaní frekvencie, vyžarovacieho výkonu a priepustnosti podľa odpovedí na požiadavku, ktorú pri zapnutí podpory IEEE 802.11d v prístupovom bode zasiela v podobe broadcastu ISO kódu krajiny, v ktorej sa AP (Access Point) nachádza, ako súčasť beacon paketov.

IEEE 802.11e

- doplnok vylepšujúci MAC podvrstvu linkovej vrstvy rozšírením podpory kvality služieb (QoS) vytvorený v roku 2005 pre normy rodiny 802.11, tento štandard je dôležitý pre aplikácie náchylné na omeškanie, napríklad prenos hlasu a videa (dáta závislé na čase), prúdové multimédiá a VoIP (Voice over Internet

Protocol). IEEE 802.11e doplňuje štandardy 802.11 a/b/g. Existujúce metódy pre prístup k médiu DCF (Distributed Coordination Function) a PCF (Point Coordination Function) sú nanovo nahradené metódami EDCF (Enchanced DCF) a HCF (Hybrid Coordination Function). Doplnok 802.11e k tomu spätne zaisťuje kompatibilitu so zariadeniami nevybavenými podporou QoS. (12)

IEEE 802.11h

- doplnok štandardu IEEE 802.11a, navrhnutý v roku 2004, a tak, aby bral ohľad na európske podmienky pre potreby využívania siete mimo budovy. Rieši problémy spojené s rušením od ostatných zariadení pracujúcich v 5 GHz frekvencii vylepšením riadenia kmitočtového spektra. Pri detekcii rušenia má za úlohu obmedziť vysielací výkon alebo uvoľniť kanál, na ktorom rozpoznal rušenie. Štandard tak upravuje fyzickú vrstvu i MAC podvrstvu linkovej vrstvy. Dynamický výber kanálu nám potom zaručuje lepšie pokrytie jednotlivých kanálov. (12)

IEEE 802.11i

- dodatok známy tiež ako WPA2 z roku 2004, ktorého predchodcom bol WPA (WiFi Protected Access), nahrádza protokol WEP (Wired Equivalent Privacy) integrovaný do IEEE 802.11. Používa metódu dočasného kľúča TKIP (Temporal Key Integrity Protocol) oproti statickým kľúčom používaným v protokole WEP. Zameriava sa na zdokonalenie zabezpečenia vylepšením autentizačného a šifrovacieho algoritmu pre bezdrôtové siete a podporou dlhších šifrovacích kľúčov, ktoré sa budú s časom meniť oproti krátkym a trvalým kľúčom používaným protokolom WEP. Použitý je nový spôsob blokového šifrovania AES (Advanced Encryption Standard) oproti predchádzajúcej prúdovej šifre RC4 pre WEP a WPA. Nová architektúra 802.11i obsahuje protokol IEEE 802.1X pre autentifikáciu, ktorý používa EAP (Extensible Authentication Protocol) a autentizačný server s štvorcestným „handshake“, RSN (Robust Security Network) pre uchovávanie záznamov o asociácii a šifrovací algoritmus AES zalo-

žený na blokovej reťazovej šifre CBC (Cipher Block Chaining), ktorý poskytuje utajenie, integritu dát a autentifikáciu.(2, s. 38)

IEEE 802.11k

- doplnok vyvinutý pre zvýšenie efektivity využitia prenosového média pomocou merania kvality jednotlivých kanálov, merania šumu, zahltenia a vzájomného rušenia kanálov. Podľa týchto meraní sa optimalizuje nastavenie klientov a sieť sa nakonfiguruje tak, aby bola dosiahnutá čo najväčšia kvalita spojenia. (12)

IEEE 802.11n

- upravuje fyzickú vrstvu a podvrstvu MAC linkovej vrstvy s cieľom dosiahnuť reálnej rýchlosti minimálne 100 Mbit/s. Maximálna rýchlosť môže byť teoreticky až 600 Mbit/s. Toho je docielené vďaka použitiu MIMO technológie, ktorá prináša vyšší dosah a väčšia dátová priepustnosť a odolnosť proti rušeniu, a to vďaka použitiu viacerých antén. Používa metódu OFDM. Vývoj IEEE 802.11n trvá od roku 2003, do roku 2008 existovalo mnoho produktov na báze IEEE 802.11n Draft 2.0. Norma bola len nedávno schválená, v roku 2009, reálne dosiahnuteľná rýchlosť je okolo 130 Mbit/s, a to je oproti iným dodatkom veľký skok dopredu. 802.11n je spätne kompatibilná s 802.11b/g, preto nie je problém s postupnou integráciou nových zariadení do bežných sietí. Problém však nastáva pri využívaní viacerých kanálov v, už i tak moc zarušenom, bezlicenčnom pásme, kvôli nemožnosti využitia týchto kanálov súčasne, a tak sa prenosová rýchlosť výrazne zníži. (13)

IEEE 802.11q

- dodatok je rezervovaný a často zamieňaný s 802.1Q VLAN (Virtual Local Area Network). (12)

IEEE 802.11v

- vytvára unifikované rozhranie pre správu zariadení v bezdrôtových sieťach. Správa sietí bude vykonávaná centralizovane alebo distribuovane pomocou mechanizmu na druhej linkovej vrstve. Zahrňuje funkcie pre monitoring a konfiguráciu sietí. (12)

IEEE 802.11w

- na MAC podvrstve linkovej vrstvy implementuje mechanizmy podporujúce integritu dát, autenticitu zdroja dát, utajenie dát a ochranu pred útokmi typu Replay. Cieľom tejto normy je zvýšenie zabezpečenia prenosu. (12)

1.7 Topológia bezdrôtových sietí

Usporiadanie a štruktúra siete môže byť prevedená dvomi spôsobmi. Rozdeľujeme topológiu sietí[3] so základným súborom služieb (BSS, Basic Service Set) a siete s rozšíreným súborom služieb (ESS, Extended Service Set). BSS sú siete pozostávajúce zo zariadení, ktoré sú vo vzájomnom dosahu alebo v dosahu jedného prístupového bodu, územie vzájomného dosahu nazývame Basic Service Area (BSA). V sieťach typu ESS sa môže väčší počet zariadení ľubovoľne prekrývať a dosiahnuť tak rozšíreného dosahu jednej siete. Môžeme povedať, že ESS sa skladá z niekoľkých BSS sietí. Sietí typu BSS existujú dva druhy, o ktorých si popíšeme nižšie.

1.7.1 Ad-hoc siete

Nazývané aj nezávislé siete typu P2P (peer-to-peer), zariadenia v nich komunikujú priamo, podľa potreby a nezávisle na prostredníkovi, neobsahujú žiadny AP. Toto schéma je vhodné pre menšiu sieť so stanicami vzdialenými od seba pár metrov, pretože pri vzájomnej komunikácii medzi sebou musia byť stanice vo vzájomnom rádiovom dosahu. (3, s. 44)

[3] BRISBIN, Shelly. Wi-fi: Postavte si svou vlastní wi-fi síť. 2003, s. 34.

1.7.2 Infraštruktúrne siete

Ich základom je jeden či viac AP, ktoré riadia komunikáciu a zabezpečenie staníc siete, stanice sú závislé na prostredníkovi – AP. Táto topológia sa hodí pre rozsiahle a trvalé bezdrôtové siete. AP môže plniť funkciu router-u či bridge. Komunikácia prebieha v dvoch fázach, dáta putujú najprv zo stanice na AP a až potom smerujú z neho na druhú stanicu. Ak je sieť zložená iba z jedného AP, jedná sa o BSS sieť, ak by sme prepojili dve a viac sietí BSS dostaneme druhý typ infraštruktúry ESS. (3, s. 46)

1.7.3 Bezdrôtové premostenie siete

Access point pracujúci v tomto špeciálnom režime môže spájať dve alebo viac sietí bezdrôtovo. Preto ich nazývame bezdrôtové mosty – Wireless Bridge, tento režim umožňuje fyzické spojenie medzi inak oddelenými sieťami i na väčšie vzdialenosti bez pomoci káblov, komunikácia prebieha medzi dvomi Access point-mi. V tomto prípade dve siete fungujú ako jedna, Access point, ktorý vytvára most môže zároveň fungovať aj ako prístupový bod a prepojiť segmenty siete aj s ostatnými bezdrôtovými zariadeniami, napr. tlačiarňou, a poskytovať tak bezdrôtový prístup do siete, AP však túto funkciu musí podporovať. (3, s. 47, 48)

Poznáme rôzne prevádzkové režimy premostenia sietí, tie sú popísané nižšie.

Point-to-Point Bridge

K vytvoreniu spojenia medzi dvomi káblovými sieťami je používaný mechanizmus Point-to-Point Bridge. Podmienkami pre používanie tohto mechanizmu je nastavenie rovnakého názvu SSID pre obe koncové zariadenia a nastavenie MAC adresy druhého zariadenia, ďalej tieto zariadenia musia operovať na rovnakom kanáli. Tu však musíme brať v ohľad skutočnosť, že Access point-y v tomto móde nie sú schopné komunikovať s inými bezdrôtovými zariadeniami, sú vyhradené len pre komunikáciu medzi dvoma sieťami, a preto ak chceme implementovať bezdrôtovú infraštruktúru, treba do návrhu včleniť samostatné prístupové body, ktoré budú vyhradené pre komunikáciu s klientskými stanicami. Takto vytvorené premostenie

sietí je jednoduché, ale pre zachovanie bezpečnosti sa odporúča zapnúť šifrovanie komunikácie a obmedzenie MAC adries. (3, s. 48)

Point-to-Multipoint Bridge

Mechanizmus Point-to-Multipoint Bridge je vhodný použiť pri premosťovaní viac ako dvoch sietí. Komunikácia prebieha medzi všetkými zariadeniami pracujúcimi v tomto režime, každý prístupový bod komunikuje s ostatnými prístupovými bodmi. Využite tohto mechanizmu je hlavne v rozsiahlych sieťach umiestnených vo viacerých budovách, alebo ak sú siete od seba vzdialené. Konfigurácia zariadení je zaistená automaticky, treba však dávať pozor na to, aby zvolené zariadenia boli od jedného výrobcu, či používali taký istý firmware, pri nezhode sa môžu vyskytnúť isté problémy spôsobené nekompatibilitou zariadení. I tu nie je možné použiť Access point-y na pripojenie klientských staníc. Bezpečnosť pri použití tohto mechanizmu môžeme zaistiť nastavením filtru MAC adries. (5, s. 47)

Repeater

Tento špeciálny režim premostenia umožňuje, aby Access point pracoval ako prístupový bod a zároveň aj ako bridge. Takýmto spôsobom môžeme rozšíriť dosah bezdrôtovej siete bez pomoci káblov. Problémom je, že nie každé zariadenie podporuje funkciu repeater-u, a tie ktoré ho podporujú patria k tým drahším, avšak treba zvážiť možnosť prakticky nekonečného rozširovania siete pomocou tohto režimu a to i v miestach, kde je rozšírenie pomocou káblov nemožné. Princíp tohto režimu spočíva v prijímaní signálu z jedného zariadenia, zosilnenie tohto signálu a následné vyslanie ku koncovému zariadeniu, týmto spôsobom dokážeme prenášať signál aj v miestach, kde vzdialenosť medzi dvomi zariadeniami je moc veľká a nemáme dobré spojenie v priamej viditeľnosti medzi anténami na oboch stranách bezdrôtového spojenia. (3, s. 50, 51)

1.8 Bezpečnosť bezdrôtových sietí

Hlavným faktorom pôsobiacim na bezpečnosť WiFi sietí je problematické teritoriálne vymedzenie pokrytia siete, tento problém u káblových siete neriešime, pretože je náročné odpočúvať prevádzku siete, je treba sa fyzicky dostať k samotným káblom. A tu vidíme prvú nevýhodu bezdrôtových sietí, kde pre odpočúvanie stačí, ak sa dostaneme do priestoru, v ktorom sa dá zachytiť signál. Samozrejme dosah bezdrôtovej siete môžeme ovplyvniť obmedzením výstupného výkonu AP, ale útočník si i tak nájde cestu, ako sa do siete dostať. Preto je dôležité si svoju bezdrôtovú sieť zabezpečiť. Vo väčšine prípadov si zákazník, ktorý si zakúpi WiFi router, sieť postaví a bez ďalších znalostí používa bezdrôtové pripojenie k internetu, sieť nezabezpečí a tým vystavuje svoje dáta riziku zneužitia, pritom si nie je vedomý tohto pochybenia. Dôležité je analyzovať, čo potrebujeme chrániť a pred čím sa potrebujeme chrániť, to znamená zistiť slabé miesta v bezpečnosti siete a analyzovať možné ciele útokov na sieť a zamerať sa na najkritickejšie a najpravdepodobnejšie z nich.

A preto ak chceme vybudovať bezpečnú sieť je treba brať ohľad na minimalizáciu zraniteľných miest a tými sú hlavne:

- **Informácie, dáta** (heslá, komunikácia, dokumenty v elektronickej podobe, atď.),
- **Služby**, ktoré zaisťujú prenos a spracovanie dát,
- **Zariadenia,**
- **Užívatelia** z hľadiska identity.

Zabezpečenie sietí môžeme rozdeliť do dvoch skupín:

- **Šifrovanie** – zamedzenie odpočúvania prenášaných dát,
- **Autorizácia** – riadenie prístupu užívateľov, povolenie a zamedzenie pripojenia

Vo firemnom prostredí prichádza na rad bezpečnostná politika, pretože informácie môžu mať niekedy väčšiu cenu než drahé kovy či umelecké dielo. Know-how a patenty, vynálezy a iné sa v dnešnej dobe uchovávajú v elektronickej podobe a sú tak vystavené možnému riziku odcudzenia. Predstavme si, že zamestnanec po-

nechá zapnutý bezdrôtový príjem na notebooku pripojenom ethernetovým káblom k lokálnej sieti v spoločnosti. Tu dostane útočník šancu na preniknutie do siete a možnosť získania citlivých informácií. Preto je dôležité stanoviť si pravidlá bezpečnosti, zabezpečiť nielen prístupové body ale aj klientské stanice, sieť samotnú, bezdrôtové zariadenia a určiť užívateľom jasné pravidlá pre používanie bezdrôtového pripojenia. Voľba bezpečnostnej politiky musí vychádzať s dostupných prostriedkov a aktuálnych požiadaviek na zabezpečenie, ktoré sme zistili dôkladnou analýzou, treba mať na pamäti pravidlo, že útočník musí vynaložiť viac na prelomenie ochrany, ako môže zo samotného prelomenia získať. (5, s. 125)

1.8.1 Bezpečnosť Wi-Fi na jednotlivých vrstvách

Bohužiaľ neexistuje dokonalé zabezpečenie počítačového systému, ale aby sme sa k tejto dokonalosti aspoň priblížili, musíme zabezpečenie realizovať po vrstvách a iba tak vytvoríme systém odolný proti útokom. Nesmieme ale zabudnúť, že ak bude mať útočník dostatok času a prostriedkov, akokoľvek silná obrana môže byť prelomená, a preto je treba vytvoriť čo najviac bezpečnostných prekážok tak, aby sme útočníka odrazili od pokusu o útok, alebo tento útok čo najviac znemožnili.

Bezpečnosť na fyzickej vrstve

Tu môžeme realizovať ochranu v rámci funkcií fyzickej vrstvy, a nimi sú:

- *Modulácia* – útok sa zakladá na použití rovnakej metódy modulácie pre úspešné odpočúvanie siete (FHSS, DSSS, ...).
- *Riešenie interferencií signálu* – zaistenie správneho smerovania antény pre usmernenie signálu použitím smerovej antény, toto zabezpečenie sa nedá dosiahnuť použitím všesmernej antény.
- *Priepustnosť dátového toku* – dosah signálu ovplyvňuje okolie, pre zabezpečenie v budove je vhodné použiť ochranné materiály na kovovej báze, fólie či nátery, v otvorených priestoroch musíme obmedziť vysielací výkon či použiť rušičky.

- *Logická identifikácia siete* – útok je možný na základe asociácie útočníka so sieťou a preto musí poznať sieťový identifikátor, štandardne SSID. (4, s. 59)

Bezpečnosť na spojovej vrstve

Medzi funkcie spojovej vrstvy patrí hlavne prepojovanie komunikácie mostmi, prepínanie a virtuálna LAN. Zabezpečenie sa týka hlavne podvrstvy MAC, kde potrebujeme riadiť a kontrolovať prevádzku a to pomocou chybového riadenia, potvrdzovania rámcov, riadenie zahltenia siete metódou CSMA/CA, šifrovaním a agregáciou paketov. Pomocou implementácie viacerých sieťových protokolov je možné filtrovať prevádzku. Overenie identity klientov môže prebiehať otvorene, bez overenia alebo pre zvýšenie bezpečnosti je možné použiť autentizáciu klientov pomocou WEP zdieľaného kľúče, pomocou protokolu 802.1x EAP, alebo s použitím autentizačného serveru, napr. RADIUS. Prevádzku v sieti je možné šifrovať, napr. pomocou WEP, DES/3DES či AES.

MAC adresa – (Media Access Control) slúži na identifikáciu klientov pre prístup k sieti, MAC adresa je jedinečný identifikátor sieťového zariadenia uložený vo firmware zariadenia, skladá sa zo 48 bitov a je zapisovaný v podobe šiestich dvojciferných hexadecimálnych čísel oddelených pomlčkou, napr. 48-2C-6A-1E-59-3D. Zoznam na základe adries MAC definuje prístupové pravidlá, filtruje klientov bez povolenia k prístupu k sieti. Výrobcom pridelená MAC adresa je vždy jedinečná. Rozdeľuje sa na dve polovice, o prvú polovicu výrobca žiada centrálneho správcu adresného priestoru a táto polovica je u tohto výrobcu rovnaká, druhej polovici priradí výrobca jedinečnú hodnotu, a tým je zaistená jedinečnosť MAC adries. Táto sa dá však zmeniť, mnohokrát priamo v zariadení cez webové rozhranie. (4, s. 60)

Bezpečnosť na sieťovej vrstve

Na tejto vrstve je dôležité zabezpečiť podporu QoS, roaming klienta, smerovanie komunikácie a riadenie prideľovania bandwidth-u. Hlavnými funkciami, ktorými môžeme zabezpečiť sieť sú:

- *Filtrácia IP adries* - pomocou zoznamu IP adries a pridelených oprávnení riadime prístup klientov.
- *Firewall* – funkcia implementovaná vo WiFi router-i, ktorá plní funkciu blokovania prenosu z Internetu do siete, slúži ako filter nebezpečného obsahu prenosu.

1.9 Obrana

Ako už bolo spomenuté vyššie, u bezdrôtových sietí sa signál šíri v priestore a mnohokrát jeho dosah zasahuje do priestoru, kde nechceme aby sa šíril. Na zabezpečenie takejto siete existuje nepreberné množstvo spôsobov na ochranu, avšak existuje i veľký počet možných útokov na tieto zabezpečovacie techniky. Ako príklad uvediem techniku, pri ktorej sa nastavuje DHCP server tak, aby prideľoval IP adresy známym MAC adresám a neznámym klientom prideľoval IP adresu rozdielnu od našej siete spolu s odlišnou maskou siete.

Bezpečnosť Access Pointu

Tu je najdôležitejšie zamedziť prístup k vzdialenej správe prístupového bodu, pretože po získaní prístupu by mohol útočník zistiť všetky potrebné informácie, použité kľúče a na základe tohto zmeniť nastavenia siete. Najlepší spôsob ako toto vykonať je povoliť správu iba prostredníctvom pripojenia metalickou sieťou, zakázať bezdrôtovú správu AP. Predpokladom je, že iba oprávnené osoby majú prístup k metalickej infraštruktúre v podniku či domácnosti. Taktiež je potrebné fyzicky zabezpečiť AP pred možnosťou resetovať ho a tak ho uviesť do továrenských nastavení, čiže bez zabezpečenia. Ak to AP umožňuje, je dobré ak sa vytvorí Virtuálna sieť LAN, kde sa nastavia užívateľské skupiny, tým sa určia prístupové práva k prostriedkom a službám siete a takto umožníme riadenie prevádzky v sieti a jej zabezpečenú správu.

Autentizácia

Proces overenia identity užívateľa, služba stanice v norme 802.11, funguje na princípe zaslania overenia existencie AP stanicou na základe prijatého broadcast-u, zaslania tzv. Probe request-u, ktorý obsahuje SSID žiadanej siete a informáciu o rýchlosti podporovanej stanicou. Na základe tohto request-u odpovie AP v dosahu zaslaním svojho SSID, ktoré sme si vyžiadali, odpovedným rámcom Probe response obsahujúcim parametre tejto siete (SSID, rýchlosť, hustota beaconov, timestamp, atď.). Ostatné AP s SSID rozličným od požadovaného tento požiadavok ignorujú, takže tento proces zaistí spojenie iba s nami požadovaným AP, po spojení sa môže klient autentizovať.

Autentizácia v sieťach so štandardom 802.11 predstavuje jednosmerný proces overenia identity, takže užívateľ musí o autentizáciu požiadať, ale sieť sa naproti tomu autentizovať voči ostatným zariadeniam nemusí. Tento princíp privileguje AP čo umožňuje útok nazývaný Man-in-the-middle, v princípe ide o vytvorenie falošného prístupového bodu medzi klientom a pravým AP. O útokoch na bezdrôtové siete si viac povieme v inej kapitole.

Autentizovať sa môžeme dvomi spôsobmi:

- **Otvorená autentizácia – Open System**

  Je implicitnou voľbou autentizácie v bezdrôtových sieťach, jej princíp spočíva na prijatí klientského zariadenia, ktoré zašle svoju identifikáciu v podobe SSID bezdrôtovej stanice, prístupovým bodom na základe overenia týchto údajov. Ak má AP povolené vysielanie SSID, môže každý klient s jeho znalosť vstúpiť do siete, pre obmedzenie prístupu do siete sa doporučuje vypnúť vysielanie SSID, kde sa pri neznalosti SSID sieť neobjaví v ponuke prístupných sietí. Zámerne píšem obmedzenie prístupu, a to preto, že aj pri vypnutom vysielaní SSID sa dá toto zistiť pomocou programov ako je *NetStumbler* a utilita operačného systému Windows XP *Zero Config*.

- **Autentizácia zdieľaným kľúčom – Shared Key Authentification**

  Základom tejto bezpečnejšej metódy je znalosť kľúča na strane klientov žiadajúcich o prístup do siete. Proces overenia identity klienta je nasledovný:

  1. klient požiada o autentizáciu, vyšle rámec 802.11 obsahujúci jeho údaje a žiadosť o autentizáciu,
  2. prístupový bod zašle výzvu (challange) v podobe náhodne vygenerovaného čísla
  3. klient výzvu zašifruje s pomocou kľúča, odvodeného zo zdieľaného autentizačného kľúča, a tú potom odošle,
  4. bezdrôtová stanica šifru dešifruje, výsledok porovná so pôvodnou výzvou, nasleduje potvrdenie úspešnosti alebo zamietnutie prístupu.

  Uvedené informácie sa v tejto metóde prenášajú otvorene, hrozí útok na odhalenie kľúča, pretože je zasielaný otvorený text a vzápätí šifrovaný text a tieto dve informácie postačujú útočníkovi k určeniu kľúča. (4, s. 21)

1.9.1 SSID

Ako už iste vieme SSID (Service Set Identifier) je identifikátor bezdrôtovej siete, implicitne je vysielaný prístupovým bodom ako *beacon* každých pár sekúnd. Pre pripojenie k určitej sieti je nutná znalosť SSID, ktorý predstavuje kľúč až o 32 znakoch, bez jeho znalosti nie je možné pripojiť klienta na bezdrôtovú stanicu.

SSID neslúži pre zabezpečenie siete, jeho utajením však môžeme užívateľom v sieti poskytnúť trochu bezpečia. Bohužiaľ dnes existuje mnoho programov, napr. NetStumbler, ktorý dokáže skryté SSID odhaliť a to dvomi spôsobmi:

1. Pasívnym odpočúvaním siete, v momente, kedy sa nejaký klient na sieť pripojí útočník SSID získa.
2. Aktívnym zasielaním odpojovacieho paketu do siete pripojeným užívateľom, tých sieť znovu pripojuje a tu sa naskytne príležitosť odpočuť SSID.

Okrem skrytia SSID efektívna ochrana neexistuje, preto je jeho skrytie najefektívnejšie v nových nepoužívaných, nenakonfigurovaných sieťach. Podobný identifikátor používaný ako nástroj pre riadenie prístupu klientov do siete, ktorý je priamo naprogramovaný priamo v AP je ESSID (Extended Service Set Identification), ten ale AP nevysiela, pripojenie do WiFi siete je povolené iba autorizovaným klientom s jeho znalosťou. Pri použití ESSID pre prístup klientov, ktorí majú znalosť hodnoty tohto identifikátoru vytvoríme uzavretú sieť. (4, s. 66)

1.9.2 MAC adresa

Riadenie prístupu do siete na základe vytvorenia zoznamu MAC adries a filtrácia týchto klientov pomoc ich MAC adries je jednou z doplnkových možností, ako zabezpečiť prístup do siete len pre autorizovaných užívateľov, zároveň je to najjednoduchší a rozumný spôsob ochrany siete pred neoprávneným prístupom. AP však pre použitie tejto metódy musí túto funkciu podporovať, čo platí vo väčšine zariadení. Slabinou je jednoduchá odpočúvateľnosť MAC adries z takto vytvorených prístupových listov a jej následné použitie v klientskom zariadení, kde sa dá hodnota MAC adresy manuálne nastaviť na želanú odpočutú MAC adresu. Ďalšou nevýhodou prístupových listov je ich zdieľanie v sieti využívajúcej roaming na všetkých AP, pretože tento zoznam musí byť na všetkých staniciach rovnaký. Tento problém sa dá vyriešiť tak, že tento zoznam umiestnime na server, kde si ho AP budú môcť stiahnuť a v prípade zmeny zoznamu postačuje previesť zmeny len na jednom mieste a tak poskytnúť zdieľanie jednotného zoznamu všetkým AP. Z uvedeného riešenia vidíme, že je vhodné použiť ho v kombinácii s RADIUS serverom, o ktorom bude napísané nižšie. (1, s. 22)

1.9.3 Šifra WEP

V cudzom názve *Wired Equivalent Privacy* predstavovala pôvodnú šifrovaciu metódu pre siete 802.11. Z názvu vyplývalo, že zámerom vytvorenia tohto protokolu bolo poskytnúť užívateľom bezpečnosť zrovnateľnú k metalickým sieťam. Vo výsledku svoj účel nesplnil, prelomenie WEP kľúča je možné za 2 minúty

s použitím správneho software, ale o útoku na WEP bude napísané v inej kapitole. Poďme sa pozrieť ako vlastne WEP funguje.

WEP používa prúdovú šifru RC4 a kontrolný súčet CRC-32 pre zaručenie integrity, kľúčový reťazec vzniká spojením IV (*Incializačného vektoru*) a kľúča. Šifrovanie sa prevedie operáciou XOR medzi otvoreným textom a kľúčovým reťazcom, dešifrovanie prebieha spätným spôsobom, kde sa na šifrovanom texte prevedie operácia XOR s kľúčovým reťazcom. Pri sile šifrovania 64 bitov je dĺžka WEP kľúča 40 bitov, IV má 24 bitov a mení sa s každým paketom. Autentizácia pomocou WEP prebieha na princípe výzva-odpoveď.

Slabiny WEP

Bohužiaľ tento protokol neobsahuje žiadny mechanizmus správy kľúčov, ich prideľovania a distribúcie. Kľúč je statický a obe strany používajú ten istý kľúč pre šifrovanie a dešifrovanie komunikácie, neexistuje možnosť jeho dynamickej zmeny, preto by mal byť často obmieňaný a v to v pravidelných intervaloch, aby sa zvýšila bezpečnosť a tak prípadnému útočníkovi sťažiť odpočúvanie a prelomenie kľúča. Mechanizmus RC4 je slabý, a preto ďalšou možnosťou ako zvýšiť zabezpečenie je použiť silu šifrovania 256 bitov, kde bude mať kľúč dĺžku 232 bitov pri nezmenenej dĺžke IV, tu znížime pravdepodobnosť úspešného prelomenia kľúča na minimum – prakticky však bude prelomenie nemožné. Avšak pri odcudzení kľúča je tento prezradený a nepomôže ani silnejšie šifrovanie.

Slabinou autentizácie výzva-odpoveď je nemožnosť overenia si autenticity AP, ten môže byť falošný. (15)

1.9.4 WPA

Alebo inak povedané *WiFi Protected Access*, ktorý oproti protokolu WEP môžeme považovať za účinnú zbraň v boji proti prienikom do bezdrôtových sietí. Tento mechanizmus je vytvorený spoločnosťou *WiFi Alliance*, spája výhody štandardu 802.11i a odstraňuje všetky doposiaľ objavené problémy protokolu WEP. Zo štandardu 802.11i prevzal mechanizmus pre šifrovanie komunikácie TKIP a takisto

mechanizmus riadenia prístupu do bezdrôtovej siete. WPA je akýmsi prechodovým mostíkom medzi WEP a 802.11i a s oboma je nezlučiteľný.

Hlavnými výhodami oproti svojmu predchodcovi WEP je použitie autentizačného protokolu *EAP*, protokolu pre šifrovanie dynamickým kľúčom *TKIP* a algoritmu pre kontrolu integrity *MIC* známeho aj ako *Michael*.

TKIP

Temporal Key Integrity Protocol je mechanizmus využívajúci algoritmus RC4 podobne ako WEP, avšak kľúč má štandardnú dĺžku 128 bitov a umožňuje použitie dynamických dočasných kľúčov oproti statickým kľúčom používaným v protokole WEP. Tento automatický mechanizmus mení dočasný kľúč každých 10.000 paketov a tým odstraňuje chybu WEP-u, kde odpočúvaním bolo možné pri dostatočnom množstve opakujúcich sa paketoch odvodiť a prelomiť kľúč. V tomto prípade nie je možné zachytiť dostatočné množstvo paketov, podľa ktorých by sa dal tajný kľúč odvodiť, pretože pre odvodenie kľúča o dĺžke 124 bitov je potrebných 700 tisíc až 1 milión paketov šifrovaných rovnakým kľúčom.

MIC – Message Integrity Check

Mechanizmus zaisťujúci nelineárnu kontrolu integrity správ, tzv. *Message Integrity Check*, navrhol ho Neil Ferguson exkluzívne pre WPA a poznáme ho aj pod názvom „*Michael*“. Princíp spočíva v kontrole prenášaných dát tak, aby znemožnil útočníkovi zmenu správ pri prenose a chráni pred útokmi opakujúcimi predošlú odchytenú komunikáciu.

Pre každý paket sa odvodí z hlavného kľúča MIC kľúč. Z tohto odvodeného kľúča, informáciách o MAC adrese odosielateľa a príjemcu sa spočíta 8 bajtová hodnota MIC a vloží sa do rámca 802.11, a ten sa nakoniec zašifruje aj spolu s kontrolným súčtom MIC vloženým medzi dátovú časť rámca a hodnotu ICV (Integrity Check Value).

V návrhu protokolu 802.11i sa predpokladalo použitie zabezpečenia bezdrôtových sietí v rôznych prostrediach, napr. domácnostiach, malých i veľkých podnikoch, preto WPA podporuje dva pracovné módy:

- **Enterprise** a
- **Pre-Shared Key.**

➢ Mód WPA – Enterprise

Uplatnenie je predovšetkým v sieťach, ktoré kladú maximálne požiadavky na bezpečnosť, napr. podnikové siete charakteristické veľkým počtom užívateľov s rôznymi prihlašovacími údajmi, použitím RADIUS Serveru, kde o autorizácii rozhoduje server, nie AP.

Autentizáciu uskutočňuje EAP-TLS (*Extensible Authentication Protocol-Transport Layer Security*), ktorý zaisťuje klientom bezpečnú komunikáciu s autentizačným serverom, systém verejných kľúčov v podobe certifikátov je samozrejmosťou. Takto sa zabezpečí overenie identity medzi užívateľom a serverom navzájom, zabraňuje útokom typu *Man-in-the-middle.*

➢ Mód WPA – Pre Shared Key (PSK)

Využitie hlavne v domácnostiach a menších podnikových sieťach, kde overenie klienta prebieha na základe overenia jeho identity prístupovým bodom, používa sa zdieľaný kľúč, ktorý AP musí poznať. AP rozhoduje o autentizácii klienta na základe ním poskytnutého kľúča, ak je kľúč správny AP klienta autorizuje k prístupu do siete. (16)

1.9.5 WPA2

Zabezpečenie známe aj ako protokol 802.11i nesúce označenie RSN – „*Robust Security Network*“, bolo vytvorené v roku 2004 a jeho predchodcom boli WEP a WPA, protokol WPA je v podstate jeho podmnožinou. Hlavným prvkom WPA2 je šifra AES, ktorá v nebola vo WPA dokončená, oproti WPA, ktorý používal RC4 je v 802.11i AES povinné, zatiaľ čo TKIP zostal iba ako voliteľný mechanizmus. Toto

zabezpečenie zamerané hlavne na autentizáciu a utajenie prenášaných dát zahrňuje autentizáciu protokolom 802.1x, šifrovací protokol CCMP (***C****ounter-mode* ***C****BC (Cipher Block Chaining)* ***M****AC (Message Authentication Code)* ***P****rotokol*) a šifru AES (*Advanced Encryption Standard*).

Zaujímavosťou je spätná kompatibilita s WEP, ktorú však WPA2 úplne nahradzuje. Predchodca WPA obsahoval len niektoré časti WPA2. 802.11i je plnou implementáciou štandardu WPA2, ktorá vyžaduje plnú hardwarovú podporu od výrobcov, hlavne kvôli šifrovaciemu algoritmu AES, ten má zvýšené nároky na výkon a bez hardwarovej podpory by nebol funkcie schopný.

Zabezpečenie AES-CCMP

Šifra AES je v protokole 802.11i oproti svojmu predchodcovi novinkou, vo WPA nebola totiž ešte dokončená. Vo WPA2 nahradila predošlú šifru RC4 a je navrhnutá podľa amerického federálneho štandardu pre spracovanie informácií *FIPS (Federal Information Processing Standards*). V tomto protokole pracuje v režime AES-CCMP, Counter-mode zaisťuje šifrovanie prenášaných dát, CBC-MAC sa stará o autentizáciu a integritu informácií predávaných pri komunikácii. Princíp šifry AES je podobný ako u RC4, rozdiel je vo veľkosti kľúča, ktorý má 128, 192 alebo 256 bitov, táto šifra je založená na algoritme Rijndael, šifrovanie a dešifrovanie je možné previesť paralelne.

Postup šifrovania je nasledovný, vstupný text rozdelíme na bloky o 128 bitoch, prvý sa XOR-uje s IV a ďalší sa XOR-uje s výsledkom operácie prvého bloku až dokým nedôjde k zašifrovaniu celého vstupného textu, počítadlo sa vynuluje, XOR-uje sa hodnota MIC a tú pridáme na koniec rámca. Takto vytvorená šifra je silnejšia, zároveň je aj náročnejšia na hardware, z toho vyplýva nekompatibilita so staršími generáciami bezdrôtových zariadení.

CCMP používa dynamické generovanie kľúčov a dokáže číslovať pakety čím zabraňuje útokom typu *Replay*. IV má 48 bitov čím sa obmedzila možnosť útočníka použiť opakujúce sa IV, tie sú očíslované (označovaný PN – Packet Number, číslo paketu).

WPA2 a autentizácia

Podobne ako u WPA môžeme i tu v protokole 802.11i pracovať v dvoch režimoch, *Enterprise* a *PSK,* ktorých princíp je podobný ako u WPA.

U **WPA2-Enterprise** je autentizácia uskutočňovaná podľa protokolu 802.1x, jej princíp spočíva vo vyžiadaní si identifikačných údajov klienta prístupovým bodom, následne prebehne výmena správ medzi autentizačným serverom a klientom, na základe ktorej sa vygeneruje MK (*Master key),* v záverečnej fáze tohto procesu vyšle server správu Radius Accept obsahujúcu MK a správu EAP Success klientovi. U **WPA2-PSK** sa overuje identity pomocou zdieľaného kľúča. V oboch režimoch prebieha autentizácia obojstranne.

Voliteľne sa u WPA2 ponúka mechanizmus *pre-authentication* čiže predbežná autentizácia. V tomto prípade môže byť klient pripojený k AP ešte pred samotným priblížením sa k nemu, a to za pomoci vyslania paketu žiadajúceho o autentizáciu dopredu, ešte v dobe, keď je zariadenie k AP pripojené. Výhodou je zníženie doby požadovanej na výmenu informácií medzi zariadeniami a tým zmenšenie oneskorenie, ktoré je dôležité pre aplikácie citlivé na omeškanie, napr. aplikácie využívajúce hlasové služby.

Správa kľúčov

Samozrejmosťou z hľadiska zabezpečenia je uchovávanie a utajenie kľúčov. Bezpečnosť vo WPA2 je zaistená obmedzením životnosti kľúčov a ich rôznorodosť a hierarchické usporiadanie, po úspešnej autentizácii sú v bezpečnostnom kontexte vytvárané dočasné kľúče, tie sa aktualizujú až do uzatvorenia tohto kontextu. Medzitým sa uskutočňuje *štvorcestný handshake,* kde sa tieto dočasné kľúče používajú pre odvodenie ostatných, tie sú použité pre šifrovanie, distribúciu či autentizáciu správ.

Napred musí byť medzi stanicou a autentizačným serverom zjednaný Hlavný kľúč **MSK** (*Master Session Key).* Ten poslúži ako základ pre odvodzovanie ďalších kľúčov. Z **MSK** sa odvodí **PMK** (*Pairwise Master Key*), z neho potom odvodíme **PTK** (*Pairwise Transient Key*). Do skupiny **PTK** kľúčov patria:

- KCK (*Key Confirmation Key*) – slúži ako doklad o vlastníctve PMK pri spájaní PMK s AP (stanicou), autentizuje komunikáciu v priebehu *handshake*-u.
- KEK (*Key Encryption Key*) – pomocou neho sa distribuuje GTK (*Group Transient Key*).
- TK (*Temporal Key*) – šifrujú sa pomocou neho dáta v TKIP a CCMP.
- TMK (*Temporary MIC Key)* – autentizuje komunikáciu.

PMK samotný sa nikdy nepoužije pre autentizáciu či šifrovanie správ, komunikácie. Jeho funkcia spočíva v generovaní ostatných dočasných kľúčov PTK.

Handshake umožňuje šifrovať prenos pomocou odvodených kľúčov, autentizovať klienta a jeho znalosť PMK, zaisťuje kľúče pre šifrovanie a overenie integrity dát a v neposlednom rade potvrdzuje výber sady šifier.

Utajenie a integrita dát

V 802.11i zaisťuje utajenie protokol TKIP, integritu poskytuje nový protokol MIC. Zmeny sa týkajú rozšírenia veľkosti IV pre zamedzenie použitia opakovaných IV útočníkom a implementácia správy kľúčov, ako už bolo opísané vyššie. (16)

1.9.6 Bezpečnostný štandard IEEE 802.1x a EAP

Môžeme ho chápať ako samostatný protokol alebo obecný bezpečnostný rámec pre LAN, ide však hlavne o nadstavbu protokolu WEP, ktorá je určená pre riadenie prístupu do siete na úrovni logických portov prístupového bodu. Cieľom je blokovať prístup neoprávnených užívateľov k segmentom LAN, 802.1x môžeme považovať za transport na spojovej vrstve pre správy autentizačného protokolu EAP vyššej vrstvy. Jeho úlohou je autentizácia užívateľov a správa kľúčov v rámci riadenia prístupu, nejedná sa však o utajenie komunikácie. Riadiť prevádzku v sieti môžeme i bez 802.1x pomocou filtrovania MAC adries, klienti sa však nebudú autentizovať, hlavne preto sa 802.1x hodí pre organizácie s veľkým počtom užívateľov, je tu potrebný autentizačný server a taktiež softwarová podpora na prístupo-

vých bodoch, čo je pre domáce využite finančne náročné a zbytočne komplikované riešenie. (2, s. 194)

Aby sme tento štandard pochopili, je potrebné vysvetliť pojmy PPP, EAP a samotný štandard 802.1x a jeho autentizačné metódy.

PPP

Alebo *Point-to-Point Protocol,* ktorý sa využíva u vytáčaného pripojenia k internetu pre autentizáciu užívateľa na konci linky ešte pred samotným prístupom. Jeho obmedzenie spočíva v autentizácii založenej na kombinácii mena a hesla.

EAP

Autentizačný protokol, ktorý rozširuje PPP, je obecnou platformou pre rôzne autentizačné metódy. EAP sa tvári ako zásuvný modul PPP a pri jeho použití môžeme vyberať z rôznych autentizačných metód a použiť tú, ktorá nám najviac vyhovuje, napr. autentizáciu heslami, certifikátmi, tokenmi, PKI, čipovými kartami, Kerberos-om, biometrikou a inými. Ak budem chcieť v budúcnosti zabezpečenie vylepšiť, stačí len vymeniť mechanizmus, pretože EAP je otvorený štandard, a tak bude možné použiť i nové ešte teraz neznáme metódy.

Autentizácia v 802.1x

Systém autentizácie je jednoduchý a je tvorený tromi komponentmi, žiadateľom, autentizátorom a autentizačnými serverom. Žiadateľom je klient, notebook či iné prenosné zariadenie. Autentizátorom je AP. Autentizačný server je akýsi zoznam klientov, ktorí majú prístup povolený.

Celé to funguje nasledovne. Medzi autentizátorom a serverom sú dva porty, jeden je riadený, ktorý slúži na prevádzku v sieti a implicitne je v neautorizovanom stave, kedy je blokovaná prevádzka. Druhú port je neriadený a ten slúži výhradne na komunikáciu serveru s autentizátorom. Žiadateľ pošle rámec *EAP Start*, výzvu k pripojeniu, autentizátor odpovie rámcom *EAP Request/Identity*, ktorým sa pýta na identitu klienta, ten pošle rovnaký rámec späť a pomocou neho sa identifikuje, au-

tentizátor túto informáciu predá serveru. Autentizačný server na to zareaguje zaslaním rámcu EAP-Request so žiadosťou na informáciu, napr. vloženie hesla, túto žiadosť autentizátor zašle žiadateľovi, ktorý na to odpovie požadovaným spôsobom, autentizátor jeho odpoveď zašle serveru. Autentizačný server overí identitu klienta a zašle autentizátorovi rámec EAP-Success alebo EAP-Failure podľa výsledku autentizácie, autentizátor po prijatí rámcu EAP-Success riadený port odblokuje a prepne do autorizovaného stavu, až potom môže prebiehať komunikácia. Autentizátor tu vystupuje ako sprostredkovateľ, klient server ani sieť nevidí, až po úspešnej autentizácii. (2, s. 195)

Autentizačné metódy v 802.1x

Protokoly 802.1x a EAP predstavujú spolu iba platformu, na ktorej je možné realizovať rôzne zabezpečené autentizačné konverzácie. Týchto metód je veľa a preto si v tomto odstavci popíšeme tie najrozšírenejšie.

- **EAP MD-5 (*Message Digest*) –** predstavuje najnižšiu formu zabezpečenia autentizácie prostredníctvom mena a hesla. Jednostranná autentizácia zo strany klienta znemožňuje overiť si identitu AP, preto je táto metóda zraniteľná útokom *Man-in-the-middle.* Celá komunikácia prebieha otvorene, bez šifrovania. Heslo musí byť na serveri uložené v podobe otvoreného textu, čo na bezpečnosti moc nepridáva, ďalej nepodporuje dynamické generovanie kľúčov. Táto metóda nie je vhodná pre použitie vo firemnom prostredí, a to hlavne pre jej nedostatočnú bezpečnosť, aj keď jej implementácia je veľmi jednoduchá. (1, s. 84)
- **EAP-TLS (*Transport Layer Security*) –** z pohľadu bezpečnosti sa jedná o najsilnejšie riešenie zabezpečenia autentizácie a komunikácie v bezdrôtových sieťach. Autentizácia je obojstranná na základe digitálnych certifikátov podpísaných certifikačnou autoritou, TLS podporuje dynamickú obnovu WEP kľúčov. Pre zabezpečenie komunikácie sa vytvára šifrovaný tunel prostredníctvom *PKI,* v ňom potom prebieha výmena autentizačných údajov. Toto zabraňuje útokom typu *Man-in-the-Middle.* Kameňom úrazu je potreba certifikátov na obidvoch stranách, čo je administratívne i finančne náročné, preto sa imple-

mentácia tohto riešenia hodí v prostredí, kde sú už klientské certifikáty zavedené. Metóda TLS bola z hľadiska zabezpečenia najsilnejšou, no existuje útok pomocou ktorého je možné komunikáciu rozlúštiť. Ten je založený na odchytávaní šifrovanej komunikácie, jej analýze a vytváraní výziev pre server na základe tejto šifrovanej komunikácie. Server na tieto výzvy odpovedá a tak poskytuje postranné informácie, z pomocou ktorých je možné šifru rozlúštiť. (1, s. 85)

- **EAP-TTLS (*Tunneled Transport Layer Security*) –** predstavuje zjednodušenú podobu TLS, používa jeho výhody v podobe komunikácie prostredníctvom zašifrovaného TLS tunelu a dynamickej generácie WEP kľúčov, ale pre vzájomnú autentizáciu vyžaduje certifikát už len na strane serveru, klient sa autentizuje pomocou hesla. Táto metóda je silnejšia ako metóda LEAP a jednoduchšia na implementáciu ako EAP-TLS. (1, s. 85)
- **PEAP (*Protected Extensible Authentication Protocol*) –** jedná sa o internetovú verziu EAP-TTLS, podporuje obojstrannú autentizáciu medzi klientom a autentizačným serverom a potrebou certifikátu len na strane serveru, pre komunikáciu sa vytvára zabezpečený kanál, ale pre autentizáciu je možné použiť i slabšiu bezpečnostnú metódu, a celý postup bude bezpečný, pretože táto komunikácia bude prebiehať v zabezpečenom tuneli. V tomto prípade autentizátor komunikáciu medzi klientom a serverom len preposiela. (1, s. 86)
- **LEAP (*Lighweight Extensible Authentication Protocol by CISCO*)** – spoločnosť Cisco v roku 2000 navrhla nový protokol vyžadujúci obojstrannú autentizáciu klienta a autentizátora prostredníctvom mena a hesla, nie je potrebné vlastníctvo certifikátov. Autentizáciu inicializuje klienta a následne na to sa inicializuje prístupový bod. Zahrňuje i dynamickú generáciu WEP kľúčov. Nevýhoda spočíva v nekompatibilite protokolu so zariadeniami od ostatných výrobcov. Ak by sme chceli LEAP implementovať, musíme mať všetky zariadenia v infraštruktúre (adaptéry, AP, server, atd.) od výrobcu Cisco. LEAP sa preto moc nerozšírilo, hlavne kvôli prevahe zmiešaných prostredí, kde sa nedá zaistiť uniformita dodávateľa sieťových prvkov. (1, s. 84)

1.9.7 RADIUS Server

V neskrátenej podobe *Remote Authentication Dial-In User Services* - bezpečnostný server na ktorý sa užívatelia prihlasujú pomocou mena a hesla, aby overili svoju identitu voči sieti a na základe ich autorizácie sa môžu do siete pripojiť a využívať jej služby, v podstate ponúka centralizovanú správu prístupu klientov do siete a pracuje na princípe klient-server. RADIUS ponúka AAA koncept riadenia prístupu do siete, to označuje ***autentizáciu (autentication)*** – identifikáciu užívateľov a riadenie prístupu do siete, ***autorizáciu (authorization)*** – definíciu prístupových práv a riadenie prístupu k službám siete a ***účtovníctvo (accounting***) – sledovanie pohybu užívateľov po sieti a sledovanie zdrojov, ku ktorým bolo pristupované z dôvodu účtovania za služby. Každý oprávnený užívateľ má vytvorený účet a svoje prihlasovacie údaje uložené na serveri v zašifrovanej podobe, každý má udelené prístupové práva k jednotlivým službám siete. Protokol RADIUS podporujú hlavne drahšie zariadenia, rozšírený je hlavne v podnikovej sfére. (14)

Autentizácia

Táto prebieha zadaním mena a hesla užívateľa, podporované metódy autentizácie sú **PAP** (*Password Authentication Protocol*) – autentizáciu inicializuje klient zaslaním svojich údajov, a **CHAP** (*Challenge Handshake Authentication Protocol*) – výzva zo strany serveru, po vzájomnej výmene informácií a odsúhlasení ich správnosti sa ustanoví spojenie. Prenos autentizačných údajov sa šifruje, heslo a meno medzi klientom a serverom putuje v šifrovanej podobe. (4, s. 81)

1.10 Útoky na bezdrôtové siete

V predchádzajúcej kapitole sme si povedali niečo o zabezpečovacích mechanizmoch bezdrôtových sietí. Každému je jasné, že naproti ním stojí celá rada útokov, ktoré majú za úlohu tieto mechanizmy prelomiť. Prečo by toto niekto robil? Odpoveď je jednoduchá, môže to byť zo zvedavosti, prelomenie zabezpečenia je pre niekoho výzvou, ďalej sú to pokusy o získanie prístupu k internetu zdarma cez susedovu nezabezpečenú WiFi sieť a v neposlednej rade sú tu útoky na firemné

siete vo forme priemyselnej špionáže s cieľom získania citlivých informácií či know-how.

Bezdrôtové siete sa priamo ponúkajú útokom, sú ideálnym cieľom z hľadiska dostupnosti, pripojiť sa na ňu môže skoro hocikto ak sieť nemá implementované silnejšie zabezpečovacie mechanizmy. Informácie sa dajú odpočúvať technikou zvanou *„sniffing“*, sledovať susedove emaily, správy komunikačných aplikácií, zachytávať heslá zadávané v otvorenej podobe alebo jednoducho analyzovať informácie prúdiace sieťou.

WiFi v poslednej dobe zažila veľký boom, skoro každá domácnosť je dnes vybavená bezdrôtovým routerom s AP. Väčšina z nich však nekladie dôraz na zabezpečenie týchto sietí, zvyknutí na metalickú sieť a majúci presvedčenie, že stačí ak si zvolíme heslo na prihlasovanie do operačného systému, zakúpia si bezdrôtové zariadenie a ako ho vybalia zo škatule, tak ho ponechajú v továrenskom nastavení. Tím otvoria bránu do svojej siete všetkým v dosahu, neškodným užívateľom i útočníkom, pre ktorých nebude problém sieť zneužiť. Nie je k tomu treba žiadnych zvláštnych znalostí alebo špeciálnych zariadení, na takto nezabezpečené siete sa pripojíte so svojim notebookom, ktorý musí mať bezdrôtovú kartu. Po pokuse o pripojenie sa do siete cez AP mu je pridelená IP adresa cez DHCP a útočník tak získa prístup, teraz nie je zložité zmeniť nastavenia siete, stačí zistiť výrobcu a typ AP. Niekedy je toto možné zistiť z SSID, ktoré už od výroby identifikuje bezdrôtové zariadenie. Potom už len stačí nájsť si na internete užívateľskú príručku, kde výrobca udáva továrenské nastavenia (predvolenú IP, prihlasovacie meno a heslo do AP), pomocou nich sa prihlásiť cez webové rozhranie do AP a veselo meniť nastavenia.

Predstavu o tom, ako sú na tom bezdrôtové siete so zabezpečením si môžeme urobiť i sami, stačí nasadnúť na jednom konci mesta na mestskú hromadnú dopravu, zobrať so sebou notebook a cesta na druhý koniec mesta monitorovať okolie pomocou softwaru ako je napr. *NetStumbler*. Zistíme, že viacero sietí je zabezpečených veľmi chabo či úplne vôbec.

V podnikateľskej sfére je na zabezpečenie braný väčší zreteľ, spoločnosti si uvedomujú cenu informácií a náležite investujú do ich zabezpečenia, do hardwaru i

softwaru ako sú firewall-y, antivírové či antispywareové programy. Hlavným komponentom zabezpečenia je kvalifikovaný správca siete, ktorý sieť analyzuje, hľadá jej slabiny a následne vypracuje návrh zabezpečenia a navrhuje bezpečnostnú politiku.

Z pohľadu podniku je najhoršie, ak útočník po prelomení zabezpečenia siete pokračuje ďalej, snaží sa získať kontrolu na sieťou, pokúša sa ovplyvniť AP, routery a servery. Ak sa takémuto útočníkovi podarí získať administrátorské oprávnenie k prístupu, jeho meno a heslo, môže zmeniť všetky nastavenia a to tak, že ani oprávnený správca siete nebude mať prístup k nastaveniam tejto infiltrovanej siete. V tomto prípade nezostáva iná možnosť ako ručne resetovať zariadenia, ako sú AP či router. Ak sa útočníkovi podarí dostať na server, môže získať či zmazať cenné dáta a tým vyradiť server a celú sieť z prevádzky.

Z týchto a iných dôvodov je nutné, aby správca siete poznal možné slabiny siete a vedel predpovedať možné útoky, poznal ich princíp fungovania a proti týmto sa vedel účinne brániť. V ďalších podkapitolách si popíšeme najpoužívanejšie útoky, ktoré môžu byť na našu sieť smerované.

1.10.1 Útok typu DoS – *„Denial of Service“*

Jedná sa o neinvazívny útok s cieľom vyradenia siete z prevádzky. Útokom DoS môžeme spomaliť komunikáciu v sieti, alebo ju úplne zamedziť, a to za pomoci zahltenia AP veľkým množstvom nezmyselných dát, ktoré musí AP vyhodnotiť, čo zahltí celé prenosové pásmo, spomalí alebo znemožní pripojenie užívateľov. Útok môžeme previesť rôznymi spôsobmi, ktoré sú:

- zahltenie siete veľkým množstvom nezmyselných rámcov,
- zaplavenie rámcami pre odpojenie zo siete,
- sfalšovaním autentizačných rámcov – rámce obsahujúce chybu spôsobia klientovi problém s opätovným pridružením k sieti,
- pri chýbajúcej ochrane šifrovaním môže útočník zasielať deasociačné a deautentizačné rámce k AP a tým zablokovať pravé pakety,

- preplnením bufferu AP, ktorý pri preplnení autentizačnými rámcami a vytvorení veľkého množstva spojení či prijatí veľkého množstva žiadostí na autentizáciu pretečie a spôsobí spadnutie prístupového bodu. Server po prijatí požiadavku na vytvorenie spojenia otvorí linku a zašle odpoveď útočníkovi, no odpoveď nedostane, takto otvorí mnoho spojení a nie je schopný obslúžiť pravých užívateľov. (9)

Ochrana proti DoS

Proti DoS existuje málo efektívnych protiopatrení, proti zahltení sa dá brániť nastavením firewall-u, povolíme na ňom iba určitý počet paketov za sekundu z jednej IP adresy. Ďalšou možnosťou je filtrovanie MAC adries.

1.10.2 Man-in-the-Middle

Útok s „mužom uprostred“, ktorý vstúpi medzi AP a klienta, odpočúva ich komunikáciu, v prvej fáze zhromažďuje dáta o klientovi i AP, informácie ako IP adresy, SSID AP či MAC adresu klienta. Dáta analyzuje a dekóduje, po získaní dostatočného počtu informácií ich komunikáciu preruší, vytvorí falošný AP, ktorý umiestni blízko užívateľa a donúti ho pripojiť sa naň. Nielenže všetku komunikáciu zachytáva, preposiela ju od klienta k AP a naopak, tí sa domnievajú, že spolu komunikujú priamo, skutočnosť je, že ich komunikácia je sprostredkovaná a zachytávaná útočníkom. Takto útočník získava všetky informácie ako sú prihlasovacie mená a heslá klienta a všetky ostatné dáta. Síce tento útok patrí k tým náročnejším, existuje veľké množstvo programov slúžiacich na uskutočnenie tohto útoku.

Ochrana proti M-I-T-M

Zabrániť sa mu dá pomocou použitia VPN či autentizačných mechanizmov ako je 802.1x, najmä tých s obojstrannou autentizáciou pomocou serveru RADIUS. Vhodné je i mapovanie signálu v okolí siete a hľadanie falošných AP, ktoré nepatria do našej infraštruktúry. (4, s. 106)

1.10.3 MAC Spoofing

Útok spočívajúci vo vydávaní útočníkovho zariadenia za iné zariadenie, ktoré má v sieti zriadené prístupové právo. Jeho využitie je v sieťach, kde je nastavená filtrácia pomocou MAC adries. Útočník teda musí zmeniť MAC adresu svojho zariadenia na MAC adresu takého zariadenia, ktorá má do siete povolený prístup. MAC adresu zariadenia si zistíme z rámcov získaných odpočúvaním komunikácie v sieti, vyhľadáme si hlavičku MAC adresy a tú prečítame, pri použitom zabezpečení WEP je treba tento najprv rozlúštiť a MAC adresu získať z rozlúštenej komunikácie. Zmena MAC adresy na zariadení je v dnešnej dobe možná priamo v nastavení samotného zariadenia napr. cez webové rozhranie.

Ochrana proti MAC Spoofing

Tomuto útoku je možné predísť použitím autentizácie cez 802.1x či použitím VPN. (5, s. 136)

1.10.4 WEP Cracking (rozlúštenie WEP kľúča)

Na prelomenie WEP je potrebných približne 5 – 10 miliónov paketov, predpokladom je, že užívateľ po dobu zberu dát WEP kľúč nezmení. Tento útok sa dá realizovať pomocou programov AirSnort či WEPCrack. Môžeme ho realizovať viacerými metódami:

- **Útok hrubou silou (*Brute-force Attack*)** – výpočtovo veľmi náročný útok, je potrebné kombinovať so slovníkovým útokom, pomocou programu od Tima Newshama je možné prelomiť touto metódou 40 bitový WEP kľúč za pár desiatok sekúnd na stroji Pentium 4, 2.6 GHz. Čím je silnejšie heslo, tým je dlhšia doba na jeho prelomenie. Existuje hardwarovo akcelerované lámanie pomocou Pico karty, ktoré umožňuje úplné prehľadanie pre 40 bitový kľúč do 34 hodín na obyčajnom notebooku.
- **Slovníkový útok (*Dictionary Attack*)** – obmedzenie počtu kľúčov v brute-force útoku na najčastejšie používané kombinácie. Tie sú uložené v slovníku so súborom pravidiel. Program tieto slová vyberá zo slovníku a postupne na nich

uplatňuje pravidlá, ktoré slová modifikujú, tie sú zašifrované a porovnané so súborom hesiel. Slovník obsahuje bežné slová, heslá ako 1234567, qwerty, password a slová z oboru a najčastejšie používané heslá.

- **Útok FMS** – páni Fluhrer, Mantin a Shamir poukázali na slabinu WEPu v algoritme plánovania kľúčov RC4. Prvý program schopný WEP prelomiť bol AirSnort uverejnený dňa 17.8.2001, odvtedy sa začalo o slabej bezpečnosti WiFi diskutovať vo veľkom. Podmienkou pre rozlúštenie kľúča WEP je zachytenie veľkého množstva paketov, kľúč je potom možné prelomiť na základe opakujúcich sa slabých paketov s unikátnym IV.
- **Útok KoreK** – dňa 8.8.2004 hacker KoreK uverejnil svoju novú metódu analýzy šifrovaných dát, pracuje s algoritmom plánovania RC4. Je potrebné zachytiť čo najviac paketov s rovnakým IV. Rozlomenie je možné už po zachytení pár sto tisícov paketov. Táto metóda je implementovaná do programov AirCrack a WepLab. (15)

Ochrana pred WEP Cracking

Chrániť sa je možné použitím 128 bitového WEP, tím znížime šancu prelomenia kľúča útokom hrubou silou. Použitím zabezpečenia RSN, čiže WPA či WPA2 zabránime tomuto útoku úplne, kľúč sa dynamicky mení a tak nie je možné ho rozlúštiť, pretože základy dešifrovania sa rozpadnú so zemnou kľúča. Proti útoku FMS je efektívne používať výlučne silné IV, neposielať slabé IV, to je zabezpečené mechanizmom WEP+, od firmy Agere Systems, ktorý je implementovaný na niektorých zariadeniach. Použitím RSN sa dokážeme obrániť i pred KoreK útokom.

1.10.5 PSK cracking (útok hrubou silou, slovníkový útok)

Útok budeme viesť na WPA/WPA2 v móde PSK. WPA neobsahuje slabiny ako WEP, integrita dát je kontrolovaná algoritmom MIC, čím sa znemožnilo upraviť zasielané správy, algoritmus TKIP zas eliminoval výskyt slabých IC, jediná slabosť spočíva v zdieľanom kľúči, ktorý je uložený na všetkých staniciach a tak celá bezpečnosť siete záleží len na sile tohto kľúča. Existuje utilita coWPAtty, ktorá

umožňuje slovníkový útok hrubou silou, lámanie hesiel o dĺžke 8-64 znakov je takmer nemožné, najmä z hľadiska času. Pri rýchlosti skúšania 50 hesiel za sekundu je možné za jeden deň vyskúšať 4.320.000 slov, možných kombinácií 8 znakového hesla je 208.827.064.576, v najhoršom prípade tak slovníkovú útok môže trvať až 48.340 dní.

Ochrana pre PSK Cracking

Osvedčenou ochranou proti tomuto útoku je použitie čo najdlhšieho a najneobyčajnejšieho hesla, ktoré bude obsahovať mix veľkých a malých písmen, čísel a znakov ako sú @, # a pod. (16)

1.10.6 Útok na LEAP

Zabezpečenie od Cisco má slabinu, ktorá bola odhalená v roku 2003 Joshuom Wrightom. Spočíva v prenose mena vo forme otvoreného textu a na overenie hesla používa algoritmus MSCHAPv2, schému challenge/response, kde je 8-bajtová výzva 3-krát nezávisle šifrovaná 56-bitovým DES (Data Encryption Standard) a následne zaslaná ako 24-bajtová odpoveď, tieto tri kľúče sa generujú za pomoci 16-bajtového MD4 hash-u, tretí kľúč sa na konci doplní o 5 nulových bajtov a preto má iba 216 možností. Preto po dešifrovaní odpovede môžeme určiť 2 posledné bajty MD4 hash-u. To nám umožní vyhľadanie v predvypočítanej tabuľke hash-ov – dešifrovaním hash-u stačí overiť iba malú časť slovníka. Tieto slovníky sú rozsiahle vďaka popularite lámania Windows hesiel a je možné ich nájsť na internete.

Ochrana pred útokom na LEAP

Ako obrana pomôže zmena autentizačnej metódy, napr. na tunelovací protokol EAP-TLS či EAP-TTLS. (16)

1.10.7 Wardriving, warwalking

Tieto techniky slúžia na zisťovanie dostupnosti sietí v dosahu buď za jazdy dopravným prostriedkom s otvoreným notebookom a zapnutým bezdrôtovým prijí-

mačom alebo počas chôdze po obci, či okolí. Zároveň pri mapovaní týchto sietí zisťujeme úroveň ich zabezpečenia, a to bez toho aby sme sa ne tieto siete pokúšali pripojiť či nejakým spôsobom siete zneužívať. Na to, aby sme takúto činnosť mohli vykonávať, nám bude stačiť notebook vybavený štandardnou WiFi kartou a operačným systémom Windows XP či Linux. V základe ide o pasívnu aktivitu zameranú na zisťovanie SSID bezdrôtových sietí

V sieťach 802.11 sa môžeme asociovať dvomi spôsobmi a to:

- **Asociáciou v otvorených sieťach**

V tomto prípade nám SSID ohlási samotný AP, ten pravidelne SSID vysiela v administratívnych rámcoch *beacons,* ktoré obsahujú aj iné dôležité informácie o sieti, podporovaných rýchlostiach a pod. My ako klient tieto rámce prijmeme a ak sa budeme chcieť asociovať, vyšleme AP žiadosť o asociáciu a ten nám na ňu odpovie jej povolením či zamietnutím.

- **Asociáciou v uzavretých sieťach**

V uzatvorených sieťach musíme hodnotu SSID poznať, ak ju nevieme, môžeme si ju s pomocou utility NetStumbler (WinXP) či Kismet (Linux) zistiť, ďalšou možnosťou je počkať si na legitímnu asociáciu iného klienta a tak hodnotu SSID odchytiť. V prípade ak nemáme ani utilitu ani čas na vyčkávanie asociácie nejakého klienta, môžeme AP zaslať požiadavku na disasociáciu, čiže odpojenie pripojeného klienta, ktorý sa vzápätí pokúsi znovu so sieťou asociovať, a tu môžeme znovu odchytiť hodnotu SSID, ktorá sa behom tohto procesu reasociácie vysiela. (1, s. 57, 58)

2 Analýza problému a súčasnej situácie

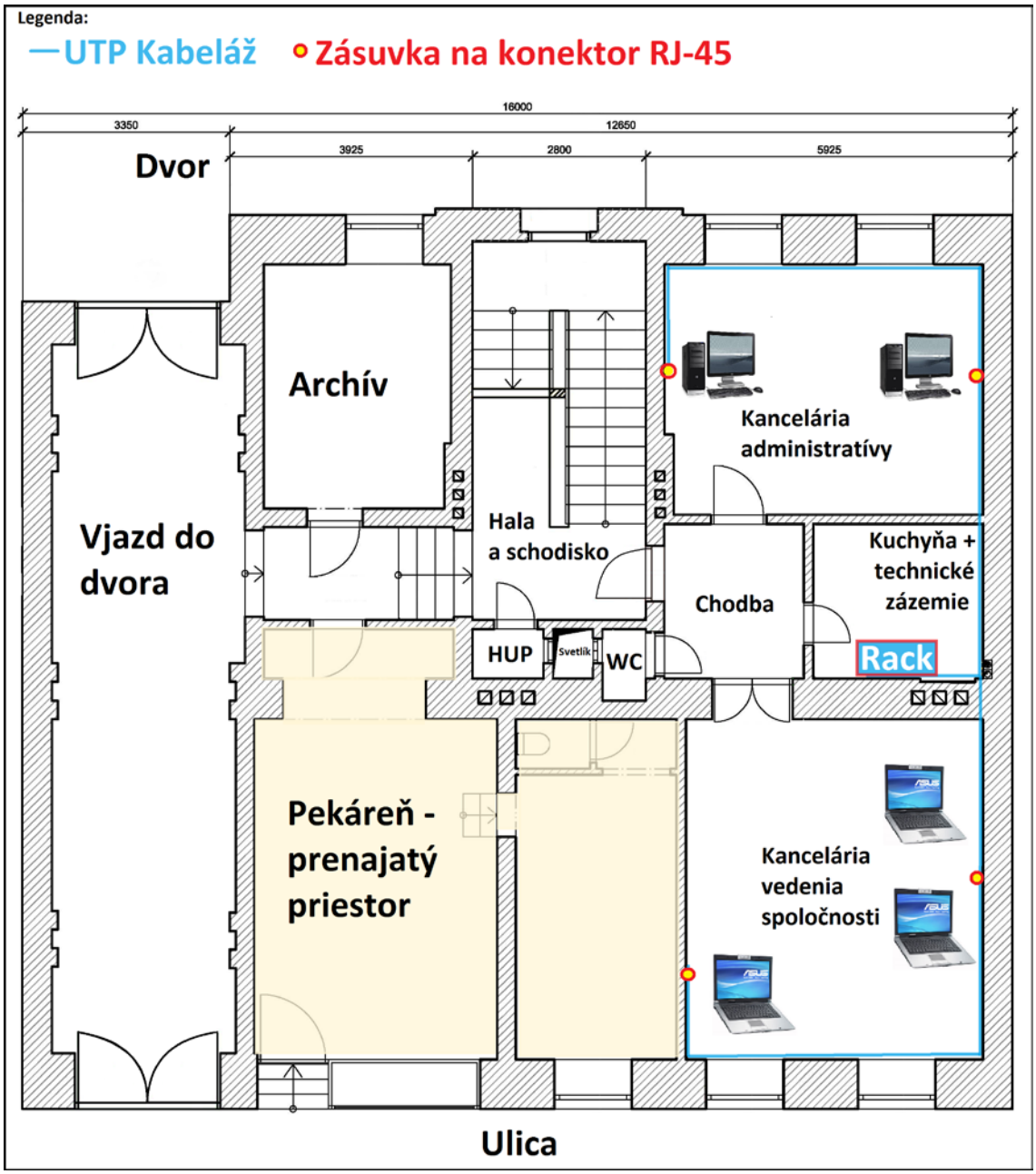
Návrh na modernizáciu, rozšírenie a zabezpečenie podnikovej siete budem vypracovávať pre spoločnosť **Dolfin AM, s. r. o.**

Spoločnosť bola založená 14. marca 2007, sídli v Brně a je zameraná na správu nehnuteľností, ich predaj, kúpu a prenájom a iné činnosti v oblasti správy nehnuteľností. Podrobné informácie o IP adresách, heslách či iné mi nebolo dovolené uverejňovať. Preto nebude možné v návrhu siete upresňovať detaily týkajúce sa nastavenia siete.

Ako aj iné technológie, tak i bezdrôtové siete zažili v posledných rokoch veľký rozmach. S pribúdajúcim počtom bezdrôtových sieťových zariadení, i technických i softwarových vylepšení a v neposlednej rade aj ich zabezpečení pribúda stále viac a viac zariadení, prostredníctvom ktorých sa môžeme do týchto sietí pripojiť a komunikovať v nich. Či už sa jedná o notebooky, PDA, tlačiarne či projektory, potreba pripájať tieto zariadenia do siete bezdrôtovo stále rastie a popri tom netreba zabudnúť na zabezpečenie takýchto spojení. A to je dôvod, prečo sa spoločnosť Dolfin AM rozhodla zmodernizovať svoju sieťovú infraštruktúru, a to hlavne jej bezdrôtové prvky, ktoré neplnia svoju funkciu a sú bez zabezpečenia. Zadanie bolo jasné, vytvoriť sieť, do ktorej budú môcť pristupovať klienti, dodávatelia či obchodný partneri spoločnosti so svojimi bezdrôtovými zariadeniami bez toho, aby sa museli ťahať po kancelárii káble, a zároveň aby bola sieť zabezpečená pred odcudzením informácií, akými sú technická dokumentácia budov, účtovnícke dáta, informácie o bankových účtoch a platobných kartách. Preto sa vo vlastnom návrhu zameriam na vytvorenie čo najbezpečnejšej siete, aby bola čo najviac nedobytná, a jej implementácia a administrácia jednoduchá. Nepoužívam zámerne výraz dokonale nedobytná, pretože neexistuje žiadna 100% bezpečná sieť, na každý bezpečnostný mechanizmus sa skôr či neskôr nájde útok, či sa odhalí nejaká slabina takéhoto zabezpečenia. Budem sa pri návrhu zabezpečenia snažiť prípadnému útočníkovi čo najviac sťažiť jeho snahu o prelomenie, či ho od pokusu o útok aspoň odradiť.

2.1 Analýza siete spoločnosti Dolfin AM, s. r. o.

Ako prvé je potrebné vykonať analýzu stávajúceho stavu siete, na základe ktorej navrhneme vhodné riešenie tak, aby sme splnili požiadavky vedenia spoločnosti.



Obrázok č. 1: Schéma stávajúceho stavu siete

Vo firme je vybudovaná metalická sieť, kabeláž je rozvedená do oboch kancelárií ako môžeme vidieť na *Obrázku č. 1*, základom siete je rack, v ktorom je umiestnený

fileserver, ktorý tvorí stolný počítač štandardnej konfigurácie s operačným systémom Windows XP na ktorom je uložený účtovnícky program Pohoda. Mailový klient je realizovaný na základe MS Outlook-u na jednotlivých počítačoch. V racku je umiestnený aj jeden WiFi router typu Huawei EchoLife HG520i, ktorý nie je nastavený, je preto nefunkčný a nepoužíva sa ako bezdrôtový AP. Ďalej sa v racku nachádza pripravený server s diskovým polom zakúpený od spoločnosti Abacus Electric, s. r. o. obsahujúci 8 hot-swap diskov v konfigurácii RAID 1, inštalovaný je operačný systém Windows Small Business Server 2008, toto riešenie však nie je využívané a jeho celkové dokončenie do finálnej podoby nikdy neprebehlo. V racku je umiestnený i switch Cisco SRW2024 o 24 ethernetových portoch, ktorý podporuje IEEE 802.1 VLAN aj IEEE 802.1x autentizáciu cez RADIUS server, ďalším zariadením je router Huawei EchoLife HG520i, štandardný router zapožičaný poskytovateľom internetového pripojenia O2, ktorý podporuje IEEE 802.11b/g, autentizáciu cez 802.1x a dokonca aj WPA2-PSK, nie je však funkčný, nastavenie bezdrôtovej siete vo webovom rozhraní nie je realizované, sieť teda bezdrôtový signál nevysiela. Rack ďalej skrýva telefónnu ústredňu Agfeo AS 200 IT napojenú na NT Aethra NT1+ TRQ2102 a všetky rozvody káblov, počítače sú spojené sieťou P2P.

Spoločnosť O2 poskytuje ADSL internet s jednou pevnou IP adresou a telefónnu linku, doména spoločnosti dolfin-re.com je zaregistrovaná u francúzskej spoločnosti Amen.fr, problémom je nedostatočná technická podpora.

Technické vybavenie užívateľov siete je nasledovné. Spoločnosť vlastní dva kancelárske počítače s operačným systémom Windows 7 Professional, ktoré boli zakúpené len nedávno. Na týchto počítačoch beží virtuálny Windows XP Professional, dôvod tohto riešenia spočíva v nekompatibilite multifunkčného zariadenia HP 3392 s operačný systémom Windows 7, kde nie je možné používať skener, takže skenovanie dokumentov prebieha cez program spúšťaný vo virtuálnom Windows XP. Tieto počítače sú k sieti pripojené pomocou zavedenej metalickej siete. Vedenie spoločnosti používa notebooky Asus UL20A, k sieti sa musia pripájať pomocou ethernetového káblu. Notebooky sú vybavené WiFi kartou s podporou 802.11 a/b/g. Používaný operačný systém je Windows 7 Professional. Ďalej má jeden z jednateľov svoj osobný notebook MacBook Pro s operačným systémom Mac

OS X, taktiež používa virtuálny Windows XP, všetci zamestnanci v spoločnosti vlastnia aj smartphone-y, napr. Blackberry Bold 9700 či Nokia E71.

Rekapitulácia stávajúceho riešenia

- firma má server, ktorý nie je dokončený, účtovnícky program *Pohoda* beží na stolnom PC, ktorý slúži ako *fileserver*,
- nie je zavedený *firewall*, žiadna filtrácia spamu, nefunkčná bezdrôtová sieť,
- vo firme je nedokončené riešenie serveru, je však ešte potrebné dokúpiť záložný zdroj, vyriešiť klimatizáciu serveru,
- management spoločnosti používa notebooky, smartphone-y, je potrebné aby sa mohli pripojiť na sieť v celej firme, zatiaľ je potrebné sa vždy pripojiť na sieť káblom, prevláda rôznorodosť operačných systémov na notebookoch,
- chýba systém pre zálohu dát, diskové pole je nainštalované, nie je však používané,
- doména je registrovaná u francúzskej autority, tu je potrebné kvôli zabezpečeniu podpory nájsť hosting domény v ČR.

Tieto dôvody a hlavne závažné nedostatky v nedokončenej implementácií riešenia serveru vyústili k potrebe celkovej modernizácie siete a vytvorenie jej zabezpečenia. Hlavným cieľom bude bezpečnosť komunikácie, integrita a bezpečnosť dát na serveri, vytvorenie siete jednoduchej na administráciu a neprekročenie stanovených nákladov na vybudovanie siete vo výške 30.000,-Kč.

3 Vlastné návrhy riešenia a ich prínos

V návrhu sa počíta s dokončením rozpracovaného serveru, nahodenie všetkých sieťových aplikácií na server, ďalej sa počíta s vytvorením bezdrôtovej siete, ktorá musí byť maximálne bezpečná a jednoduchá na správu a zavedenie.

Ciele návrhu

- dokončiť server do štádia, kde budú všetky aplikácie nahodené na plnohodnotnom serveri, ktorý bude zabezpečený proti útokom typu DoS a podobným, proti výpadku prúdu, bude realizovaná záloha dát na záložný disk – RAID 1 na diskovom poli, zavedený firewall a záložný zdroj,
- pokrytie kancelárií spoločnosti Dolfin AM, s. r. o. bezdrôtovým signálom, firma sídli v jednej budove, bude treba vybudovať bezdrôtovú sieť, do ktorej sa užívatelia dostanú iba z priestorov sídla, toto bude zabezpečené:
    1. presným nastavením parametrov AP,
    2. vhodným umiestnením AP a nasmerovaním jeho antény,
    3. nastavením rozsahu vysielania a výkonu antény,
    4. zmenou parametrov SSID, zamedzenie jeho vysielania, atď.,
    5. vytvorenie 2 oddelených sietí pomocou dvoch pevných IP adries, do jednej bude autentizácia pomocou RADIUS serveru protokolom EAP-TTLS k prístupu do vnútornej siete a dátam na serveri, druhá sieť bude oddelená a bude poskytovať návštevníkom spoločnosti prístup k internetu,
    6. po obvodových stenách budovy budú nasmerované rušičky, bude treba nastaviť rovnaké SSID a MAC adresu, vysielanie na určitom kanále a frekvencii, na ktorej bude AP vysielať, tento kanál potom smerom von z budovy rušiť, tak aby nikto z vonku nemohol sieť ani „vidieť“ ani sa na ňu pripojiť,
- výber vhodných zariadení pre zaistenie vysokého štandardu bezpečnosti, výkonu, kompatibility, jednoduchosti implementácie a administrácie.

3.1 Technická špecifikácia riešenia

Navrhované riešenie bude realizované na základe štandardu IEEE 802.11g pre zabezpečenie najvyššej možnej prenosovej rýchlosti, maximálna prenosová rýchlosť 54Mb/s bude pre naše účely postačujúca, ďalej bude použitý autentizačný protokol 802.1x, ktorý poskytne riadenie prístupu užívateľov a ich bezpečný prístup k službám lokálnej siete a zabezpečenú komunikáciu v tejto sieti. Základom pre celý návrh bude zapojenie prichystaného serveru s diskovým polom. Server pracuje pod operačným systémom Windows SBS 2008, zaisťuje služby DHCP, DNS, VPN, FTP a plní úlohu fileserveru. Počítače pripojíme do domény Windows, tá bude zrealizovaná v rámci serveru a nadefinovaná v doménovej službe Active Directory, jej názov bude dolfin-re.local. Počítače budú mať názov pc1.dolfin-re.local a pc2.dolfin-re.local, notebooky pre zmenu nb1.dolfin-re.local až nb3.dolfin-re.local. K prístupu do siete bude potrebné nastaviť užívateľské účty, k VPN sa potom budú užívatelia autentizovať pomocou týchto užívateľských účtov. Typ diskového pola bude RAID 1, zrkadlovo uložené dáta dostatočne zabezpečia server proti strate dát. Všetky programy, účtovnícky software POHODA, autentizačný server, mailový server a ostatné umiestnime na novo zapojené diskové pole. Autentizácia cez RADIUS server bude realizovaná vo Windows SBS 2008.

U poskytovateľa internetu O2 bude potrebné objednať ešte jednu pevnú IP adresu, aby sme mohli lokálnu sieť rozdeliť. Je možné objednať iba balíček ďalších štyroch IP adries k našej jednej IP adrese, dostaneme tak spolu 5 pevných IP adries za cenu 479,-Kč mesačne. U ostatných poskytovateľov sú ceny podobné, napr. u UPC stojí jedna pevná IP adresa 202,-Kč mesačne, čo pri dvoch je skoro to isté.

Starý fileserver môžeme odpojiť a ponechať si ho ako záložný server pre prípadný výpadok nového serveru a diskového pola. Ako prvé musíme zakúpiť router, ktorý obsahuje kvalitný firewall, tento router bude slúžiť pre lokálnu internú sieť. Ďalej je treba kúpiť AP, ktorý bude slúžiť ako prístupový bod a druhý, ktorý splní funkciu autentikátora pre server RADIUS. WiFi router Huawei podporuje autentizáciu cez RADIUS, my však potrebujeme, aby autentikátor – AP podporoval zároveň i možnosť regulácie výkonu antény, preto musí zakúpený prístupový bod

podporovať ako aj autentizáciu pomocou 802.1x, tak i reguláciu výkonu antény a zároveň i podporu WPA2. Router Huawei môžeme použiť pre druhú sieť, ktorá bude slúžiť na pripojovanie ostatných užívateľov či zákazníkov spoločnosti iba k internetu. Ďalšou položkou bude záložný zdroj pre server, ktorý poskytne ochranu siete a zariadeniam pred výpadkom elektrickej energie a pred elektrickým skratom, aby sme predišli poškodeniu hardware-u. Posledným zariadením, ktoré bude voliteľnou voľbou pre zvýšenie zabezpečenia siete bude rušička, tú vytvoríme z obyčajného bezdrôtového prístupového bodu tak, že nastavíme SSID siete na rovnakú hodnotu ako SSID autentikátora, takisto i MAC adresu zmeníme na rovnakú a v neposlednej rade bude potrebné nastaviť rovnaký vysielací kanál, aby sme spoľahlivo rušili vysielanie signálu von z budovy.

Router pre internú sieť

Pre router sa rozhodovalo medzi typom ZyXEL Prestige 661HW-D3 a ZyXEL Prestige 660HW-T3v2, ich výber bol prevedený na základe ich nízkej ceny a veľkého množstva funkcií a čo je najdôležitejšie, v cenovej kategórii do 2.000,- Kč obsahujú veľmi kvalitný firewall. Porovnanie ich parametrov je zjavné z *Prílohy č. 1*. Ako môžeme vidieť, parametre jednotlivých zariadení sú podobné, najdôležitejšími z nich, ktoré rozhodli o výbere routeru **ZyXEL Prestige 661HW-D3** boli podpora 802.11g+ pre zaistenie vyššej rýchlosti, možnosť odpojiť anténu, podpora nastavenia pravidiel smerovania a správy paketov a v neposlednom rade i fakt, že tento router má novší chipset poskytujúci lepšiu stabilitu zariadenia. Rozhodli lepšie parametre oproti druhému routeru pri skoro rovnakej cene.

Autentikátor

Ako autentikátor bolo treba vybrať bezdrôtový router s podporou protokolu 802.1x, zabezpečenia WPA2, možnosťou regulácie výkonu antény a samozrejme za čo najvýhodnejšiu cenu. Výber padol na zariadenie od výrobcu **Asus WL-320gP**, ktorý všetky uvedené požiadavky spĺňa a jeho cena sa pohybuje okolo 4.500,-Kč. (8)

Záložný zdroj

Ďalšou položkou bude záložný zdroj, po zrelej úvahe elektrickej spotreby a náročnosti serveru na energiu som zvolil **APC Smart-UPS X 1000VA Rack/Tower LCD 230V,** ktorý poskytuje udržanie prevádzky pri 50% zaťažení serveru na 23,8 minúty, pri zálohovaní dát a 100% zaťažení serveru poskytuje prevádzku na 8,1 minúty. (7)

Rušičky

Rušičky budú realizované nákupom dvoch bezdrôtových prístupových bodov od výrobcu **TP-LINK TL-WA701ND**, ktoré musia mať smerovú anténu. (17)

Preto bude potrebné dokúpiť 2 kusy smerovej antény **TP-LINK TL-ANT2406A** a tie stávajúce na AP vymeniť. Tieto smerové antény majú vyžarovací uhol 45° v horizontálnom i vertikálnom smere, preto bude musieť byť nastavená ich presná pozícia a taktiež i parametre AP. Takto vytvorené rušičky sú jednoducho nastaviteľné a cenovo výhodné. (6)

Software

Ako autentizačný server zvolíme implementáciu NPS vo Windows SBS 2008. Tu bude treba nastaviť autentikátora, čiže prístupový bod, oprávnených užívateľov, samotný autentizačný server a pravidlá prístupu do siete. Nemusíme tak zakúpiť ďalší software, pretože tento operačný systém s podporou autentizácie voči RADIUS serveru už spoločnosť vlastní, a jeho nastavenie je jednoduché. Z hľadiska administrácie je toto riešenie najlepšie, pridanie nových užívateľov sa prevedie priamo v utilite pre správu serveru, kde nie je potrebná žiadna špeciálna znalosť.

Ďalším softvérom, ktorý bude zavedený je MS Exchange, emailový server pomocou ktorého bude v spoločnosti vedená elektronická pošta, ten je súčasťou Windows SBS 2008.

3.2 Rozpočet návrhu

Náklady na výstavbu siete uvádzam v *Tabuľke č. 1*. Položky uvedené v rozpočte zaistia spoločnosti vysokú úroveň bezpečnosti a zároveň ušetria ďalšie finančné prostriedky vzhľadom k jednoduchosti administrácie tohto riešenia. Na druhej strane je cena zakúpených zariadení, suma 22.598,- Kč ani zďaleka nedosiahla hodnotu informácií, ktoré budú chránené týmto vybavením. I z finančného hľadiska je preto voľba tohto riešenia výhodná, pretože jeho cena nepresiahla hodnotu informácií, ktoré bolo treba zabezpečiť pred odcudzením. Najdrahšou položkou je záložný zdroj, ktorý je iba doplnkom celkovej bezpečnosti sieťovej infraštruktúry.

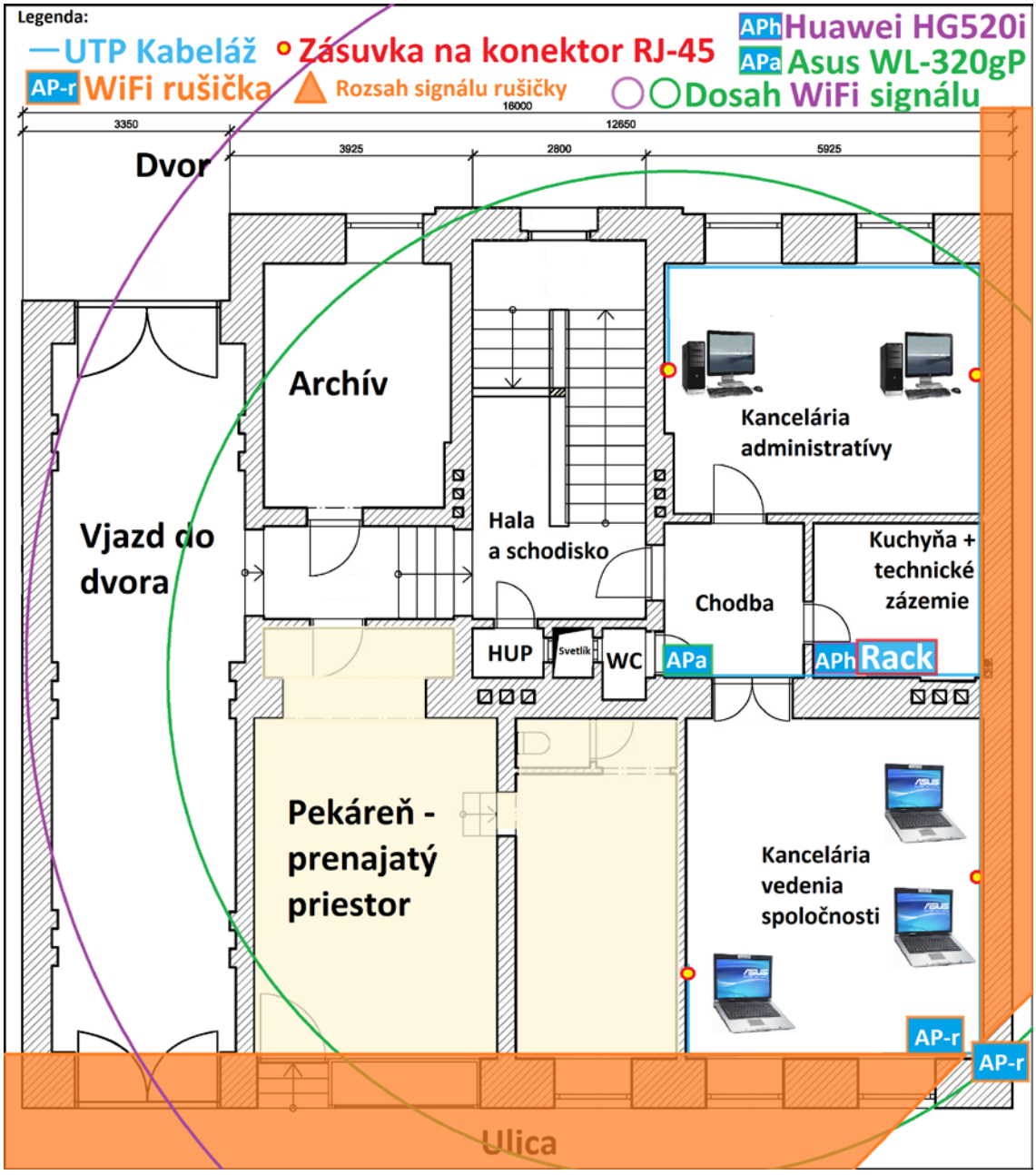
Náklady na výstavbu siete firmy Dolfin AM, s. r. o.			
Položka	**Približná cena za jednotku [Kč]**	**Množstvo [ks]**	**Cena celkom [Kč]**
Router *ZyXEL Prestige 661HW-D3*	**1 .910,-**	**1**	**1.910,-**
AP *Asus WL-320gP*	**4.500,-**	**1**	**4.500,-**
Záložný zdroj *APC Smart-UPS X 1000VA Rack/Tower LCD 230V*	**12.600,-**	**1**	**12.600,-**
Rušička *TP-LINK TL-WA701ND*	**560,-**	**2**	**1.120,-**
Anténa rušičky *TP-LINK TL-ANT2406A*	**234,-**	**2**	**468,-**
Pomocný materiál *(UTP kabeláž, koncovky a iné)*	**2.000,-**	**1**	**2.000,-**
CELKOM			**22.598,-**

Tabuľka č. 1: Náklady na výstavbu siete

3.3 Plán infraštruktúry

Schéma navrhovanej siete je zobrazená na *Obrázku č. 2*. Na znázornenom návrhu je vidieť, že bude potrebné rozviesť kabeláž UTP i do chodby, kde umiestnime prístupový bod Asus, pomocou ktorého sa budú autentizovať užívatelia do internej siete voči RADIUS serveru, na obrázku ako APa. Prístupový bod Huawei, na obrázku ako APh, ponecháme v racku, nebude záležať na jeho umiestnení, pôjde o koncový bod, kde nebude možný prístup k interným dátam spoločnosti. Keďže

chceme zabrániť šíreniu signálu od AP Asus, bude potrebné v kancelárii vedenia spoločnosti umiestniť zakúpené AP TP-LINK, na obrázku ako AP-r, ktoré budú slúžiť ako rušičky, ich antény budú nasmerované smerom von z budovy tak, aby kopírovali obvodové steny budovy a zabránili tak signálu prenikať z kancelárie do iných budov či na ulicu, kde by bolo možné signál odpočúvať.



Obrázok č. 2: Schéma návrhu siete

V priechode a na dvore nebude treba signál rušiť, dosah signálu obmedzíme tak, ako je znázornené v *Obrázku č. 2*, pokryjeme tak všetky kancelárie spoloč-

nosti a ostatný signál obmedzíme rušičkami. Ostatné sieťové prvky ponecháme na svojom mieste, zmení sa len nastavenie a niektoré z nich sa pripoja k sieti, o tom si ale napíšeme až v nasledujúcom odstavci. To ako bude prevedené zapojenie zariadení v racku je znázornené v *Prílohe č. 2*.

3.4 Nastavenie zariadení a zabezpečenie siete

Hlavnou zmenou v novom návrhu siete bude rozdelenie siete pomocou dvoch IP adries, ako môžeme vidieť v *Prílohe č. 2*.

1. sieť – AP Huawei

Prvá sieť bude takto oddelená od serveru a druhej siete, prístupovým bodom bude zariadenie Huawei HG520i, sieť bude slúžiť k prístupu dodávateľov či zákazníkov spoločnosti k internetu, nastavíme SSID na „Dolfin“, cez webové rozhranie nastavíme zabezpečenie zdieľaným kľúčom WPA2 a heslo pre túto sieť sa bude každý mesiac obmieňať, a to z dôvodu filtrácie starších užívateľov, pre zjednodušenie bude heslo zložené z názvu spoločnosti, aktuálneho mesiaca a roku, tvar napr. „DOLFINmay2011“. Z dôvodu oddelenia tejto siete nie je potrebné tento AP ďalej zabezpečovať, AP bude preto slúžiť aj na odvedenie pozornosti od hlavného prístupového bodu. Potrebné bude nastaviť pevný vysielací kanál tak, aby sa siete nerušili, táto sieť bude teda komunikovať na 1. kanáli.

2. sieť – AP ZyXEL

Druhá sieť bude slúžiť pre interné účely zamestnancov spoločnosti. Sieť bude v prvom rade zabezpečená nastavením firewallu na smerovači ZyXEL P661HW-D3, ten bude vykonávať kontrolu paketov a zabezpečovať prevenciu proti útokom DoS a DDoS a v tejto sieti bude slúžiť iba ako router, vysielanie bezdrôtového signálu na ňom vypneme, poprípade odstránime i anténu. Ďalej bude potrebné nastaviť prístupový bod Asus WL-320gP, ktorý bude plniť funkciu autentikátora do internej siete. SSID nastavíme na „RADIUS“, zamedzíme jeho vysielanie, zvolíme vysielací kanál, AP bude operovať na 11. kanáli, povolíme overovanie identity uží-

vateľov protokolom 802.1x a RADIUS serverom, zvolíme zabezpečenie WPA2 a zdieľaný kľúč, IP adresu serveru a porty, cez ktoré bude prebiehať komunikácia medzi AP a serverom, takto pripravíme AP, aby fungoval ako autentikátor. Ďalej vytvoríme zoznam povolených MAC adries, kde budú nadefinované všetky bezdrôtové zariadenia zamestnancov spoločnosti napr. notebooky Asus, zapneme ich filtrovanie a posledné nastavenie sa bude týkať vysielania signálu. Obmedzíme výkon antény a to tak, aby sme dosiahli pokrytie iba v priestoroch spoločnosti, metódou warwalking budeme sledovať úroveň a dosah signálu v priechode do dvora spoločnosti a na dvore, ak už signál v týchto priestoroch nezistíme a bude možné sa pripojiť na sieť z kancelárií, ponecháme nastavenie výkonu antény na tejto hodnote.

RADIUS

Autentizácia do siete bude prebiehať voči RADIUS serveru pomocou nastavenia NPS vo Windows SBS 2008 prostredníctvom existujúcich užívateľských účtov autentizačnou metódou PEAP s WPA2 zabezpečením a šifrovaním AES, preto je potrebné nastaviť ako AP tak i samotný server a hlavne nainštalovať certifikát, ak chceme použiť metódu PEAP.

Najprv nainštalujeme Certifikačné služby pridaním úlohy cez Server Managera, tu vyberieme možnosť *Active Directory Certificate Services*, týmto povolíme CA generovať a podpísať certifikáty pre našu doménu. V ďalšom kroku si zvolíme certifikačnú autoritu a pridáme odporučené služby potrebné pre webový zápis CA, klikneme na *Ďalší*, čiže ďalšie. Budeme vyzvaný k voľbe typu nastavenia certifikačného úradu, zvolíme *Podnikový*, následne na to budeme vyzvaný k voľbe typu CA, tu zvolíme *Koreňový CA*, klikneme na *Ďalší*. V nasledujúcom kroku budeme musieť nastaviť súkromný kľúč, zvolíme možnosť vytvoriť nový a presunieme sa k ďalšiemu kroku, kde nakonfigurujeme šifrovanie pre CA, ponecháme predvolené nastavenia, zvolíme názov certifikátu a určíme dĺžku jeho platnosti a presunieme na koniec celého procesu. Takto nastavíme CA a môžeme požiadať o certifikát potrebný pre PEAP autentizáciu. To prevedieme tak, že do príkazového riadku vo Windowse napíšeme „MMC“, tým otvoríme *Microsoft Management Console* konzolu pre správu systému kde si o certifikát zažiadame a nainštalujeme ho na náš server,

v menu konzole pôjdeme do *Súbor>Pridať/Odobrať modul snap-in,* v zobrazenom okne vyberieme *Certifikáty,* zvolíme *Pridať* a v nasledujúcom okne vyberieme možnosť správy modulu pre počítačové účty, ďalej vyberieme miestny pc, na ktorom máme konzolu spustenú, stlačíme *OK* a tým vytvoríme konzolu miestnych certifikátov, túto môžeme pre budúcu potrebu uložiť. V položke *Certifikáty(Účet miestneho pc)>Osobné>Certifikáty* klikneme na ne pravým tlačidlom, zvolíme *Všetky úlohy>Žiadosť o nový certifikát,* v zobrazenom okne potvrdíme výber stlačením tlačidla *Ďalší,* vyberieme doménu a na konci procesu stlačíme *Zapísať,* týmto spôsobom sme si vygenerovali certifikát, ktorý bude použitý pre identifikáciu nášho serveru.

Teraz sa môžeme vrhnúť na nastavenie RADIUS serveru. Znovu si otvoríme Server Managera a zvolíme službu *Network Policy and Access Services,* v ďalšom okne zaklikneme služby NPS a RRAS, potvrdíme stisknutím *Ďalší* a na koniec zvolíme *Install.* Tým sme nainštalovali služby sieťových pravidiel, pre ich nastavenie musíme v menu štart v príkazovom riadku spustiť nps.msc, otvoríme tým NPS MMC konzolu, v okne vyberieme možnosť *RADIUS server for 802.1X Wireless or Wired Connections,* v tejto časti konzole stlačíme *Configure 802.1x* pre nastavenie autentizácie cez 802.1x, v ďalšom okne vyberiem typ pripojenia 802.1x, zvolíme voľbu bezdrôtové pripojenia *Secured Wireless Connections,* nasleduje voľba autentikátora, ktorý je v našom prípade Asus WL-320gP, bude potrebné nastaviť jeho meno, IP adresu a zdieľaný kľúč, všetko potvrdíme a presunieme sa k okne, kde bude na výber autentizačná metóda, my zvolíme metódu PEAP a pred posunom na ďalší krok je potrebné túto metódu nakonfigurovať, stlačíme *Configure,* vyberieme náš certifikát a potvrdíme. Dostávame sa tak k nastaveniu užívateľských skupín, my zvolíme overovanie identity pre všetky užívateľské účty, ktoré sa budú do siete pripájať bezdrôtovo. Klienti, ktorý nebudú mať pridelené meno a heslo do siete sa tak nebudú môcť bez ich znalosti pripojiť a tým sa zvýši bezpečnosť celej siete a zabezpečí prístup len pre autentizovaných užívateľov. Stlačíme *Next* a na koniec *Finish* na dokončenie celého sprievodcu, tým dokončíme celú inštaláciu. Teraz máme aktivovanú autentizáciu užívateľov voči RADIUS serveru vo Windows SBS 2008.

Rušičky

Doplnkovým zabezpečením budú rušičky, tie zrealizujeme nasledovne. Umiestnime ich po obvodových stenách budovy tak, ako je to zobrazené v *Obrázku č. 2,* ich antény nasmerujeme smerom von z budovy a nastavíme vysielací kanál, na akom operuje prístupový bod Asus WL-320gP, čiže na 11. kanál a tým vyrušíme vysielanie signálu smerom navonok. Ďalej nastavíme rovnakú MAC adresu a SSID ako má AP Asus, tým dosiahneme rušenie práve našej druhej siete, a pri prípadnom pokuse o zachytenie signálu zvonku útočník prioritne zachytí falošný signál z rušičky, alebo AP Huawei a nie z prístupového bodu Asus, rušička tak postaví pred druhú sieť nepriepustnú barikádu, nebude tak možné pripojiť sa na internú sieť odinakiaľ, ale iba z priestorov spoločnosti.

Užívatelia

Posledné čo bude potrebné nastaviť pre úspešnú autentizáciu užívateľov voči RADIUS serveru je konfigurácia samotných bezdrôtových klientov. Notebooky používajú Windows 7 Professional a tam musíme nastaviť pripojenie k sieti ručne, predvolené nastavenie nám pripojenie neumožní. Automaticky sa nepripojíme i preto, že sieť nevysiela svoje SSID a tak ju nebude možné ani vidieť. Na klientskom zariadení je potrebné si otvoriť *Centrum sieťových pripojení a zdieľanie,* tam zvolíme možnosť *Nastaviť nové pripojenie či sieť.* Otvorí sa nám okno, v ktorom vyberieme možnosť *Ručne pripojiť k bezdrôtovej sieti.* Tu nastavíme názov siete „RADIUS“, typ zabezpečenia WPA2-podnikové, a typ šifrovania AES, zaškrtneme možnosť *Vytvorenie pripojenia automaticky* a *Pripojiť, i keď sieť práve nevysiela,* potvrdíme stlačením *Ďalší* a v ďalšom okne, ktoré nám hovorí, že sieť bola úspešne pridaná stlačíme voľbu *Zmeniť nastavenia pripojenia,* zobrazí sa okno, kde v záložke *Zabezpečenie* zvolíme metódu overovania v siete na „PEAP“ a klikneme na tlačidlo *Nastavenie,* v otvorenom okne zaškrtneme *Overiť certifikát serveru,* ďalej zvolíme server, koreňovú CA a voľby potvrdíme. V nastaveniach vlastností siete ešte klikneme na *Spresniť nastavenie,* tam zadáme režim overovania *Overenie užívateľa.* Týmto spôsobom nakonfigurujeme aj ostatné bezdrôtové zariadenia, ktoré budú do siete pristupovať.

3.5 Ekonomické zhodnotenie návrhu

Navrhované riešenie ponúka vysokú úroveň bezpečnosti, od zabezpečenia signálu až po autentizáciu užívateľov a ponúka komplexné riešenie ako zabezpečiť malú firemnú sieť. Toto riešenie je čo sa týka implementácie jednoduché a administratívne nenáročné, boli použité moderné zariadenia s množstvom užitočných funkcií, ktoré sú v návrhu plne využité, tak aby bolo riešenie efektívne. Preto budú dodatočné náklady na administráciu nulové, pretože správu siete zaisťuje pre spoločnosť Dolfin AM, s. r. o. technik, ktorý bude spravovať nové sieťové riešenie tak ako doteraz, a to za nezmenenú cenu. Celkové náklady na zavedenie navrhovaného riešenia sú nasledovné:

- **investícia do zariadení (podľa Tabuľky č. 1)** 22.598,-Kč
- **mesačné náklady za ďalšie IP adresy** 479,-Kč

Prínosom je zaistenie mobility užívateľov v sieti, a zároveň zachovanie bezpečnosti komunikácie zariadení v novo vytvorenom bezdrôtovom prostredí, ďalším prínosom je odbúranie závislosti užívateľov na pripojení svojich zariadení pomocou káblov, kde pri zvýšenom počte zariadení nebolo možné zapojiť všetky do siete. Prínos vidím i v zabezpečení prístupu k interným dátam spoločnosti, kde nebude možný prístup pomocou bezdrôtovej siete k týmto informáciám bez znalosti užívateľského mena a hesla.

Mnou navrhované riešenie je vhodné pre zavedené firemné siete s nedostatočným zabezpečením, kde je už infraštruktúra zavedená, ale chýbajú bezpečnostné prvky, toto riešenie môžu využiť spoločnosti, ktoré z dôvodov organizačných či iných potrebujú zvýšiť zabezpečenie. Týka sa to hlavne spoločností, ktoré zmodernizovali svoje technické vybavenie, rozšírili svoju sieť o moderné bezdrôtové zariadenia, ale zabudli tomu uspôsobiť zabezpečenie siete. Je treba myslieť na to, že riešenie bolo navrhnuté pre špecifické podmienky, a preto, ak by sa malo implementovať v inom prostredí, je potrebné prispôsobiť toto miestnym požiadavkám.

Záver

Ak by som mohol napísať pár slov k záveru, rád by som poznamenal, že tak ako i iné technológie, i bezdrôtové siete a ich zabezpečenie sú stále vo vývoji, vždy príde nejaké nové technické vylepšenie, vzápätí na to sa objaví nejaká jeho slabina, na ktorú bude potrebné vymyslieť záplatu či bezpečnostné riešenie. A preto bude vždy priestor na vylepšovanie a zdokonaľovanie tejto, dnes už neodmysliteľnej technológie, ktorá nám každý deň pomáha v práci i domácnosti. I to je dôvod, prečo sa treba bezpečnosti týchto sietí venovať, pretože tá nám poskytuje istotu a pocit nedotknuteľnosti v dnešnej kybernetickej džungli.

Na záver by som rád skonštatoval, že mnou navrhnuté riešenie splnilo cieľ, ktorý bol stanovený na začiatku, a teda vytvorenie bezpečnej bezdrôtovej siete s požiadavkou na maximálne prihliadnutie na jej bezpečnosť a požiadavky vedenia spoločnosti. Navrhované riešenie spĺňa ako podmienku bezpečnosti, tak i podmienku na jednoduchosť administrácie siete a stanovených nákladov. Dúfam teda, že moja práca pomôže i ostatným zorientovať sa v problematike bezdrôtových sietí.

Zoznam použitých zdrojov

Literatúra

(1) BARKEN, Lee. Wi-Fi: Jak zabezpečit bezdrátovou síť. 1. vyd. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

(2) BRISBIN, Shelly. Wi-fi: Postavte si svou vlastní wi-fi síť. 1. vyd. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.

(3) KÖHRE, Thomas. Stavíme si bezdrátovou síť Wi-fi. 1. vyd. Brno: Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

(4) PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. 1. vyd. Brno: CP Books, 2005. 179 s. ISBN 80-251-0791-4.

(5) ZANDL, Patrick. Bezdrátové sítě WiFi: Praktický průvodce. Dotisk 1. vyd. Brno: Computer Press, 2006. 190 s. ISBN 80-7226-632-2.

Elektronické zdroje

(6) *Anténa směrová TL-ANT2406A 2.4GHz 6dBi Indoor +1m pigtail | WiFi.ASPA.cz* [online]. c2011 [2011-05-29]. Dostupné z WWW: <http://wifi.aspa.cz/antena-smerova-tl-ant2406a-2-4ghz-6dbi-indoor-1m-pigtail-z101485/>.

(7) *APC Smart-UPS X 1000VA Rack/Tower LCD 230V (COMPOS DISTRIBUTION)* [online]. c2011 [2011-05-29]. Dostupné z WWW: <http://www.compos.cz/apc-smart-ups-x-1000va-rack-tower-lcd-230v_d231063.html>.

(8) *Asus WL-320gP WiFi Access Point - Wi-Fi, Routery a AP, 2,4GHz - SUNTECH Computer* [online]. 2011 [2011-05-29]. Dostupné z WWW: <http://www.suntech.cz/produkt/48671/Asus-WL-320gP-WiFi-Access-Point.htm>.

(9) HALLER, Martin. *Denial of Service (DoS) útoky: úvod* [online]. 5.9.2006 [cit. 2011-05-29]. Dostupné z WWW: <http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/>.

(10) *IEEE 802.11, The Working Group Setting the Standards for Wireless LANs* [online]. 2010 [cit. 2010-11-30]. Dostupné z WWW: <http://www.ieee802.org/11/>.

(11) PETERKA, Jiří. *Báječný svět počítačových sítí, část XXIV: Wi-Fi* [online]. 1.4.2007 [cit. 2011-05-29]. Dostupné z WWW: <http://www.earchiv.cz/b07/b0400001.php3>.

(12) *Přehled doplňků standardu IEEE 802.11* [online]. 30.12.2005 [cit. 2010-11-30]. Dostupné z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2005113002>.

(13) SIMANDL, Martin. *IEEE 802.11n - Jak na rychlé Wi-Fi doma i venku* [online]. 17.3.2010 [cit. 2010-11-30]. Dostupné z WWW: <http://pctuning.tyden.cz/hardware/site-a-internet/16921-ieee-802-11n-jak-na-rychle-wi-fi-doma-i-venku?start=6>.

(14) *Součásti infrastruktury RADIUS* [online]. c2011 [cit. 2011-05-29]. Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc757652%28WS.10%29.aspx>.

(15) ŠUSTR, Matej. *Bezpečnost a Hacking WiFi (802.11) - 3. WEP* [online]. c2007 [cit. 2011-05-29]. Dostupné z WWW: <http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-3-wep>.

(16) ŠUSTR, Matej. *Bezpečnost a Hacking WiFi (802.11) - 4. část WPA a WPA2* [online]. c2007 [cit. 2011-05-29]. Dostupné z WWW: <http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-4-%C4%8D%C3%A1st-wpa-wpa2>.

(17) *TP-LINK TL-WA701ND - ALFA COMPUTER | ALFA.cz* [online]. c2011 [2011-05-29]. Dostupné z WWW: <http://www.alfacomp.cz/php/product.php?eid=1051400872Z9000TWA>.

(18) *Wifi* [online]. 2010 [cit. 2010-11-30]. Dostupné z WWW: <http://clanky.katalogmobilu.cz/slovnik-pojmu-mobilni-telefony/1430-wifi/>.

Zoznam použitých skratiek

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DFIr	Difused Infrared
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
FMS	Fluhrer-Mantin-Shamir
IEEE	Institute of Electrical and Electronics Engineers
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MIC	Message Integrity Check
MIMO	Multiple- Input Multiple-Output
MMC	Microsoft Management Console
NAS	Network Access Server
NPS	Network Policy Server
NT	Network Termination
OFMD	Orthogonal Frequency Division Multiplexing
P2P	Peer-to-Peer
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PPP	Point-to-Point Protocol
PTMP	Point to Mutipoint
PTP	Point to Point
QoS	Quality of Services
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RRAS	Routing and Remote Accesss Services
SBS	Small Business Server
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TLS	Transport Level Security
TTLS	Tunneled Transport Level Security
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

Zoznam objektov

Tabuľky

Obrázky

Prílohy

Príloha č. 1: Porovnanie parametrov routerov ZyXEL

Príloha č. 2: Schéma zapojenia zariadení v racku